PRICE RMB 560 YUAN
（Volume Ⅰ，Volume Ⅱ）

ISBN 978-7-5352-3854-2
9 787535 238542 >

DCABES 2007 PROCEEDINGS
Editor in Chief Guo Qingping
Associate Editor in Chief Guo Yucheng
Volume I

2007 International Symposium on
Distributed Computing and Applications to
Business, Engineering and Science

DCABES 2007

PROCEEDINGS

Volume I

Editor in Chief Guo Qingping
Associate Editor in Chief Guo Yucheng

Hubei Science and Technology Press, Wuhan China

2007 International Symposium On Distributed Computing and Applications To Business, Engineering and Science

DCABES 2007 PROCEEDINGS

Volume I

Editor in Chief: Guo Qingping
Associate Editor in Chief: Guo Yucheng

Yichang, China

August 14-17, 2007

Hubei Science and Technology Press, Wuhan, China

图书在版编目(CIP)数据
2007 年电子商务、工程及科学领域的分布式计算和应用国际学术研讨会论文集 / 郭庆平、郭羽成 主编.
--武汉: 湖北科学技术出版社,2007.8
ISBN 978-7-5352-3854-2
Ⅰ.2… Ⅱ.郭… Ⅲ.分布式计算机-计算机应用-国际学术会议-文集 Ⅳ.TP338.8-53
中国版本图书馆 CIP 数据核字(2007)第 112318 号

Organized by
WUT Wuhan University of Technology

Co-organized by
CAA Computer Academic Association of Hubei Province & Wuhan Metropolis

Sponsored by

WUT Wuhan University of Technology
MOE Ministry of Education, China
NSFC National Nature Science Foundation of China

DCABES 2007 PROCEEDINGS
Editor in Chief :**Guo Qingping,** Associate Editor in Chief: **Guo Yucheng**
Editorial Production by **Wu Ruilin, Tang Jie;** Cover Art Production by **Da Min, Wan Xiaofen**
Published by ***Hubei Science and Technology Press, Wuhan, China*** Tel: +86-(0)27-87679468
Address: The 13th Floor of Block B, 268 Xiongchu Avenue, Wuhan, Post Code: 430070 P. R. China
Printed in Wuhan, China by Youngster Union Printery, Post Code: 430063
880mm×1230mm sixteenmo 71.5 sheets 1 500 k Characters First Edition August 2007
First Impression September 2007

ISBN 978-7-5352-3854-2 Price RMB 280 Yuan

QoS of Book Printing and Bounding is guaranteed by the printery.

CONTENTS

Volume I

Distributed/Parallel Algorithms

Distributed/Parallel Applications

Network Techniques and Applications

Distributed System Architectures

Software Architecture/ Parallel Programming Language

Distributed Operating System Techniques

Network/Web Security

Neural Network Computing

Volume II

Cluster Computing, Parallel Processing and Grid Computing

Multi-agent Application

Distributed Database and Data Mining

Web Service Applications and Web-based Computing

E-Commence Techniques and Applications

E- Education

Graphics, Image, Vision and Voice Processing

Embedded System, Hardware Design and Diagnosis

PREFACE

The DCABES is a community working in the area of Distributed Computing and its Applications in Business, Engineering, and Sciences, and is responsible for organizing meetings and symposia related to the field. The DCABES 2007 is the Sixth International Conference on Distributed Computing and Applications for Business, Engineering and Sciences held on 14-17 August 2007 in the Three Gorges, Yichang, Hubei, China. It is the third time for the DCABES international conference to be organized by School of Computer Science and Technology, Wuhan University of Technology.

As in previous conferences, the DCABES intends to bring together researchers and developers in the academic field and industry from around the world to share their research experience and to explore research collaboration in the areas of distributed parallel processing and applications.

In recent years, more and more attentions have been put on to the distributed parallel computing. I am confident that the distributed parallel computing will play an even greater role in the near future, since distributed computing resources, once properly cooperated together, will achieve a great computing power and get a high ratio of performance/price in parallel computing. In fact the grid computing is a direct descendent of the distributed computing.

We are gratified that the DCABES 2007 has received more than 500 papers submission，which cover a wide range of topics, such as Grid Computing, Mobile Computing, Parallel/Distributed Algorithms, Image Processing and Multimedia Applications, Parallel/Distributed Computational Methods in Engineering, System Architectures, Networking and Protocols, Web-Based Computing & E-Business, E-Education, Network Security and various types of applications etc.

All papers contained in this Proceedings are peer-reviewed and carefully chosen by members of Scientific Committee and external reviewers. Papers accepted or rejected are based on majority opinions of the referees. All papers contained in this Proceedings give us a glimpse of what future technology and applications are being studied in the distributed parallel computing area in the world.

I would like to thank all members of the Scientific Committee, the local organizer committee, the external reviewers for selecting papers. Special thanks are due to Professor, Dr. Choi-Hong LAI, who co-chaired the Scientific Committee with me. It is indeed a pleasure to work with him and obtain his suggestions.

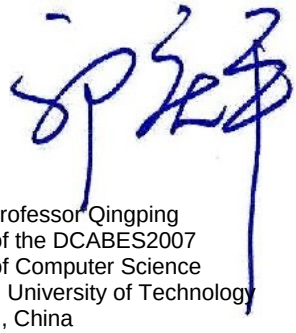
Also sincere thanks should be forward to Mr Tsui Y M Thomas, Chinese University of Hong Kong, Professor Xu W.B., Southern Yangtze University for their enthusiastically taking part in and supporting the DCABES conference.

I am also grateful to Prof. Souheil Khaddaj, Kingston University, London, UK.; Prof. V.P. Kutepov, Moscow Power Engineering Institute (Technical University), Russia; Prof. A J Davies, University of Hertfordshire, UK; Prof. Xiao-ChuanCai, University of Colorado at Boulder, USA; Prof. Choi-Hong Lai, University of Greenwich, London, UK for their contributions of keynote speeches in the conference.

Sincerely thanks should be forwarded to the Natural Science Foundation of China (NSFC), the China Ministry of Education (MOE), without their supports the DCABES 2007 could not be held in China successfully. We would also like to thank the WUT (Wuhan University of Technology, China), the National Parallel Computing Society of China (NPCS), the ISTCA (International Science and Technology Cooperation of Hubei Province, China), and the CAA (Computer Academic Association of Hubei Province & Wuhan Metropolis, China) for their supports as local organizers of the conference.

Finally I should also thank A/Professor Jian Guo for his efforts in conference organizing activities. The special thanks also should be given to my graduate students, Mr. Shadi Ibrahim for the conference website design, Mr. YeTian Li, Liang Huang and ZhiChao Yan for their efforts in organizing activities. It also should be mentioned that my graduate students, Mr YeTian Li, Liang Huang, HaiXiong An, Ms LiangLiang Wang, Yang Yang, Lin Chen, PengPeng Duan, Mr. YongQin Jia, Zhen Zhou, YuZhong Chao of the grade 2005; Mr. ZhiChao Yan, Peng Cui, Ms JuanJuan Zhao, Mr. Lin Hu, Wei Tang, GuangYou Zhou, YiFan Huang, Fan Yang of the grade 2006 spent a lot of time and efforts typesetting the proceedings. Without their help the proceedings could not looks so good.

Enjoy your stay in Three Gorges of the Yangtze River, China. Hope to meet you again at the DCABES 2008.



Guo, Professor Qingping
Chair of the DCABES2007
Dept. of Computer Science
Wuhan University of Technology
Wuhan, China

COMMITTEES

Honorary Chair
Zhou, Professor Zude, President of the WUT, China

Chair of Scientific Committee
Guo, Professor Q. P., Wuhan University of Technology

Co-Chair of Scientific Committee
Lai, Dr. Choi-Hong, University of Greenwich

Chair of Organizer Committee
Guo, Professor Q. P., Wuhan University of Technology

Steering Committee
Guo, Professor Q.P. (Co-Chair) Wuhan University of Technology, Wuhan, China
Lai, Professor C.-H. (Co-Chair) University of Greenwich, UK
Tsui, Thomas. Chinese University of Hong Kong, Hong Kong, China
Xu, Professor W.B. Southern Yangtze University, Wuxi, China

Scientific Committee (in alphabetical order)
Cai, Professor X.C. University of Colorado, Boulder, U.S.A.
Cao, Professor J.W. R&D Centre for Parallel Algorithms and Software,Beijing, China
Chi, Professor X.B. Academia Sinica, Beijing, China
Guo, Professor Q.P. Wuhan University of Technology, Wuhan, China
Ho, Dr. P. T. University of Hong Kong, Hong Kong, China
Jesshope, Professor C. University of Amsterdam, the Netherlands
Kang, Professor L.S. Wuhan University, China
Keyes, Professor D.E. Columbia University, USA
Lai, Professor C.-H. University of Greenwich, UK
Lee, Dr. John. Hong Kong Polytechnic, Hong Kong, China
Liddell, Professor H. M. Queen Mary, University of London, UK
Lin, Dr. H.X. Delft University of Technology, Delft, the Netherlands
Lin, Dr. P. National University of Singapore, Singapore
Loo, Dr. Alfred Hong Kong Lingnan University, Hong Kong, China
Ng, Professor Michael, Baptist University of Hong Kong, China
Pan, Professor Yi, Computer Science, Georgia State University, Atlanta, USA
Sloot, Professor P.M.A. University of Amsterdam, Amsterdam the Netherlands
Sun, Professor J. Academia Sinica, Beijing, China
Tsui, Mr.Thomas Chinese University of Hong Kong, Hong Kong, China
Xu, Professor W.B. Southern Yangtze University, Wuxi, China
Zhang, Professor Jun. University of Kentucky, USA
Zhou, Professor Jun, Computing Math, Chinese University of Hong Kong

Local Organizing Committee
Zhou, Professor Z.D. (Honorary Chair)
President of Wuhan University of Technology, Wuhan, China
Guo, Professor Q.P. (Chair) Wuhan University of Technology, Wuhan, China
Zhong, Professor L . (Co-Chair) Wuhan University of Technology, Wuhan, China
Liu, Professor Q. Wuhan University of Technology, Wuhan, China
Xu, Professor H.Z. Wuhan University of Technology, Wuhan, China
Chen, Professor H. Wuhan University of Technology, Wuhan, China
Xu, Professor N. Wuhan University of Technology, Wuhan, China
Zeng, Professor C.N. Wuhan University of Technology, Wuhan, China
Zhang, Professor H. M. Wuhan University of Technology, Wuhan, China
He, Professor Y. X. Wuhan University, Wuhan, China
King, Professor Hai, Hua Zhong University of Science and Technology, Wuhan, China
Tan, Professor L.S. Central China Normal University, Wuhan, China
Kang, Professor L.S. Wuhan University, Wuhan, China
Lu, Professor J.G. South Central China Nationality University

Secretary

Mr. Guo Yucheng, Wuhan University of Technology, Wuhan, China

Editorial Board

Distributed/Parallel Algorithms

Laplace Transform Time Domain-Decomposition for Diffusion Problems

A J Davies , D Crann
School of Physics, Astronomy and Mathematics, University of Hertfordshire
Hatfield, Hertfordshire, AL10 9AB, UK
Email: a.j.davies@herts.ac.uk

ABSTRACT

In most processes for the solution of parabolic diffusion problems the time derivative is handled using a finite difference approach. An alternative approach is to use the Laplace transform in time to obtain an elliptic problem in the transform space. The resulting problem may be solved using any appropriate elliptic solver. The Laplace transform approach provides a natural time domain-decomposition for diffusion problems and may be used for both linear and non-linear problems.

Keywords: Laplace Transform, Time Domain-Decomposition, Diffusion Problems.

1. INTRODUCTION

Diffusion processes are used to model a variety of problems in engineering and physical science. Such models occur in heat transfer [1] [2] and mass transfer [3]. More recently such equations have been used to model situations in biological science [4] and finance [5]. We shall consider only problems defined in a two-dimensional region, Ω, bounded by the closed curve Γ and described by the partial differential equation

$$\nabla^2 u = \frac{1}{\alpha}\frac{\partial u}{\partial t} + h(x,y,t) \quad \text{in} \quad \Omega \tag{1}$$

subject to suitable boundary conditions on Γ and an initial condition of the form $u(x,y,0) = u_0(x,y)$. Eq. (1) is often called the diffusion-reaction problem [6].

The simplest finite difference method for the time derivative in equation (1) yields an elliptic equation of the form [7]

$$\nabla^2 U^{k+1} = \frac{1}{\alpha\Delta t}\left(U^{k+1} - U^k\right) + f\left(x,y,t_k,U^k\right) \tag{2}$$

and many authors have used Eq. (2), or a variation, for the solution of linear, non-linear and coupled problems [8] [9].

An alternative to the finite difference approach is to use the Laplace transform and a detailed description may be found in references [10] and [11].

Suppose that

$$\bar{u}(x,y;\lambda) \equiv \mathcal{L}[u(x,y,t)] = \int_0^\infty e^{-\lambda t} u(x,y,t)\,dt$$

is the Laplace transform of *u*, then Eq. (1) becomes

$$\nabla^2 \bar{u} = b(x,y;\lambda) \tag{3}$$

where $b = \frac{1}{\alpha}(\lambda\bar{u} - u_0) + \bar{h}$ and $\bar{h} = \mathcal{L}[h]$. If h is a non-linear function then particular care is required for the Laplace transform and we shall describe the approach in Section 2. Eq. (3) may be solved by any suitable elliptic solver to find an approximation, $\bar{U}$, to $\bar{u}$. The difficulty associated with the Laplace transform approach is the inversion of $\bar{U}$ to find *U*, the approximation to *u*. For diffusion problems the Stehfest inversion method [12] has been shown to provide excellent results [11]. The method was first used with a finite difference solver [13] then with a finite element solver [14] and a boundary element solver [15]. The Stehfest method for the numerical inversion is given as follows:
Choose a discrete set of transform parameters

$$\lambda_j = j\frac{\ln 2}{T} \qquad j = 1, 2, \ldots, M \quad (M \text{ even})$$

then

$$U(x,y,T) \simeq \frac{\ln 2}{T}\sum_{j=1}^{M} w_j \bar{U}(x,y;\lambda) \tag{4}$$

with

$$w_j = (-1)^{\frac{M}{2}+j} \sum_{k=\left\lfloor\frac{1}{2}(1+j)\right\rfloor}^{\min\left(j,\frac{M}{2}\right)} \frac{(2k)!\,k^{\frac{M}{2}}}{\left(\frac{M}{2}-k\right)!\,k!\,(k-1)!\,(j-k)!\,(2k-j)!}$$

The attraction of the Laplace transform approach is that we obtain the solution at time T without the necessity for intermediate values as required by the finite difference method and this gives an inherent domain-decomposition approach [16] [17] [18]. Also, there is no stability problem as there is associated with the finite difference method [19].

2. THE LAPLACE TRANSFORM BOUNDARY ELEMENT METHOD

The boundary element method is now well-established as a solver for elliptic boundary-value problems [20] [21[[22]. The essence for the approach is to replace the partial differential equation boundary-value problem by an equivalent integral equation. Frequently this integral equation is defined on the boundary thus reducing the number of space variables. The technique requires a fundamental solution [23] and the use of Green's theorem to obtain the integral equivalent of equation (3) as

$$c_i\bar{u}_i + \int_\Gamma \bar{q}^*\bar{u}\,d\Gamma - \int_\Gamma \bar{u}^*\bar{q}_i\,d\Gamma + \int_\Omega b\bar{u}^*\,d\Omega = 0 \tag{5}$$

where *i* is some fixed point on the boundary, $q = \frac{\partial u}{\partial n}$ and $\bar{u}^* = -\frac{1}{2\pi}\ln R$, the fundamental solution for the Laplace operator, ∇^2. The boundary, Γ, is divided into a number of elements defined by a set of *N* nodal points and a relationship is set up between the unknown nodal values $\bar{U}_j$ and $\bar{Q}_j$. If $b \equiv 0$ then the domain integral in Eq. (5) is zero and the problem is defined only on the boundary. If $b \neq 0$ then the domain integral may be transformed to a boundary integral by the use of the so-called dual reciprocity method [24]. In this approach we introduce a further set of *L* internal points and the function $b(x,y,\bar{u};\lambda)$ is expanded in terms of a set of interpolation functions as

$$b \simeq \sum_{j=1}^{N+L} \alpha_j f_j(R) \tag{6}$$

The functions in Eq. (6) are usually taken from the family of radial basis functions [21]. The values of the coefficients α_j are found by collocation at the $N+L$ points. The functions,

f_j, are chosen in such a way that they may be related to particular solutions, $\hat{\bar{u}}_j$, of Poisson's equation, $\nabla^2\hat{\bar{u}}_j = f_j$.

The effect of the dual reciprocity approach is to obtain a system of algebraic equations of the form

$$\mathbf{H}\bar{\mathbf{U}} - \mathbf{G}\bar{\mathbf{Q}} = \mathbf{R} \qquad (7)$$

where the vectors $\bar{\mathbf{U}}$ and $\bar{\mathbf{Q}}$ contain both the unknown values of $\bar{U}$ and $\bar{Q}$ and the known values according to the prescribed boundary conditions. For properly-posed problems [25], at each point on the boundary only one of $\bar{U}_i$ or $\bar{Q}_i$ can be specified and we have in Eq. (7) an $N \times N$ system comprising *N* unknowns which may be written in the form $\mathbf{Ax} = \mathbf{y}$ [11].

For the transformed Eq. (3) the unknown $\bar{u}$ occurs in the domain function, *b*, and so the vector $\mathbf{R}$ in Eq. (7) also depends on the unknown vector $\bar{\mathbf{U}}$. The details of the dual reciprocity method lead to a relation of the form $\mathbf{R} = \mathbf{R}_1 + \mathbf{R}_2\bar{\mathbf{U}}$ where $\mathbf{R}_1$ and $\mathbf{R}_2$ are vectors which depend only on the geometry and once again we have a linear system of the form $\mathbf{Ax} = \mathbf{y}$ [11].

Non-linear problems require a linearisation prior to the use of the Laplace transform and Zhu [10] suggests a variety of approaches. The approach which has been found to be successful is a direct iteration approach in which we write Eq. (1) in the form

$$\nabla^2 u_m = \frac{1}{\alpha}\frac{\partial u_m}{\partial t} + h\left(x, y, t, u_{m-1}\right)$$

and use the Laplace transform as described above. The process is started with $u_m = u_0$ and iterated in Laplace space until convergence to within a suitable tolerance is reached. The inversion is then effected in the usual manner.

A natural domain-decomposition for the Laplace transform is obtained by associating each time value with a given processor and then obtaining the solutions in parallel.

3. APPLICATIONS OF THE DOMAIN DECOMPOSITION APPROACH

Computational finance
The Laplace transform approach is attractive because it provides an environment in which the solution may be obtained at any given time value without the need for earlier values. Problems associated with derivatives and options are modelled using the Black-Scholes equation [5]. Problems such as these in the financial sector are particularly relevant because they seek values at one time only, the time of expiry of the option [26] [27] [28]. The applications show the scalability of the Laplace transform approach and its advantage over the finite difference method.

Diffusion problems
The boundary element method has been shown to be very well-suited to a space domain-decomposition approach [29]. The so-called multipole method is currently very successful [30] and these approaches exploit an inherent parallelism in the integral formulation of boundary-value problems.
The versatility of the Laplace transform boundary element method was shown using an implementation on a sixty-four processor *nCube* machine [31] where the authors show perfect linear speed-up as would be expected because there is no inter-processor communication, except for an initial broadcast and a final gather of data. It is interesting to compare the boundary element solution with a finite difference technique in the space variables [32]. The finite difference approach uses an iterative technique for the solution of the linear equation and the convergence depends on the time, *T*. Consequently speed-up is less than linear as *T* increases.

Non-linear problems
Problems with time discontinuities in the data are handled very efficiently using the Laplace transform approach [32] [33]. Problems involving periodic boundary conditions, although strictly not non-linear, exhibit similar properties to those for discontinuous data and can be handled in a similar manner [34]. The Laplace transform is used to find the solution up to the discontinuity and this solution is used as the initial value for the post-discontinuity solution. Problems with material non-linearisation such as temperature dependent thermal properties are also handled effectively [35] [36].

An interesting non-linear problem occurs in the isotherm migration method [37] which is particularly useful for the solution of Stefan problems in which we have a moving phase-change front. The Laplace transform approach has been seen to be appropriate for such problems [38] and may be applied in a time domain-decomposition manner. Again the approach leads to linear speed-up.

Coupled problems
Some models of ocean mixing problems involve the biharmonic diffusion equation, $\nabla^4 u = \frac{1}{\alpha}\frac{\partial u}{\partial t}$, and this may be written as a pair of coupled diffusion problems [39] in a similar manner to that for solving coupled electromagnetic heating problems [40]. The Laplace transform can also be used for such problems.

Hybrid problems
A recent application of the Laplace transform method has been to allow a time domain-decomposition in a hybrid sense. A coarse-grained solution is developed over a set of time slabs and this solution is used as the initial condition for a fine-grained solution in each slab [41]. A finite difference scheme is used in each slab and since there is no interprocessor communication it yields linear parallel speed-up. [42].

4. CONCLUSIONS

The Laplace transform approach provides an excellent time domain-decomposition for parabolic diffusion problems. The solution is developed at each time-value with no requirement for the knowledge of intermediate values thus providing an independent set of solutions. The process may be applied to linear and non-linear problems. The resulting elliptic problem in transform space may be solved using any appropriate solver and the boundary element method has been shown to be particularly suitable.

REFERENCES

[1] Jakob M, Heat transfer, John Wiley and Sons, 1949.

[2] Carslaw H S and Jaeger J C, *Conduction of Heat in Solids*, 2nd ed., Oxford University Press, 1959.
[3] Crank J, *The mathematics of diffusion*, Oxford University Press, 1975.
[4] Edelstein-Keshet L, *Mathematical models in biology*, McGraw-Hill, 1988.
[5] Wilmott P, Howison S and Dewynne J, *The mathematics of Financial Derivatives*, Cambridge University Press, 1995.
[6] Logan J D, *An introduction to nonlinear partial differential equations*, John Wiley and Sons, 1994.
[7] Curran D A S, Cross M and Lewis B, *Solution of parabolic differential equations by the boundary element method using discretization in time*, Appl. Math. Modelling, Vol. 4, 1980, 398-400.
[8] Davies A J and Honnor M E, "Boundary element methods for transient and non-linear field problems", *Engineering Analysis with Boundary Elements*, Vol. 28, 2004, 561-570.
[9] Davies A J, Toutip W and Bartholomew-Biggs M C, "The dual reciprocity method for coupled thermal/electromagnetic problems", *BETECH2001*, 2001, 371-380.
[10] Zhu S-P, *Time-dependent reaction-diffusion problems and the LTDRM approach, Boundary Integral Methods, Numerical and Mathematical Aspects*, ed. Goldberg M, 1999, 1-35, Computational Mechanics Publications.
[11] Crann D, *The Laplace transform boundary element method for diffusion-type problems*, PhD thesis, University of Hertfordshire, UK, 2005.
[12] Stehfest H, "Numerical inversion of Laplace transforms", *Comm. ACM*, Vol. 13, 1970, 47-49 and 624.
[13] Moridis G J and Reddell D L, "The Laplace Transform Finite Difference (LTFD) Method for Simulation of Flow through Porous Media", *Water Resources Research*, Vol. 27, 1991, 1873-1884.
[14] Moridis G J and Reddell D L, "The Laplace Transform Finite Element (LTFE) Numerical Method for the Solution of the Groundwater Equation", paper H22C-4, ASGU91 Spring Meeting, *EOS Trans. of the AGU*, Vol. 72, 1991, 17.
[15] Moridis G J and Reddell D L, "The Laplace Transform Boundary Element (LTBE) Numerical Method for the solution of diffusion-type problems", *Boundary Elements XIII*, eds. Brebbia C A and Gipson G S, 83-97, Elsevier, 1991.
[16] Davies A J, Crann D and Mushtaq J, "A parallel implementation of the Laplace transform BEM", *Boundary Elements XVIII*, eds. Brebbia C A, Martins J B, Aliabadi M H and Haie N, 213-222, Computational Mechanics Publications, 1996
[17] Davies A J, Mushtaq J, Radford L E and Crann D, "The numerical Laplace transform solution method on a distributed memory architecture", *Applications of High Performance Computing V*, eds. Power H and Long J J, 245-254, Computational Mechanics Publications, 1997.
[18] Crann D, Davies A J and Mushtaq J, "Parallel Laplace transform boundary element methods for diffusion problems", *Boundary Elements XX*, eds. Kassab A, Brebbia C A and Chopra M, 259-268, Computational Mechanics Publications, 1998.
[19] Smith G D, *Numerical solution of partial differential equations: finite difference methods*, Second edition, Oxford University Press, 1978.
[20] Brebbia C A, Telles J C F and Wrobel L C, *Boundary Element Techniques*, Springer-Verlag, Berlin and New York, 1984.
[21] Wrobel L C, *The Boundary Element Method Volume 1*, Wiley, 2002.
[22] Aliabadi M H, *The Boundary Element Method Volume 2*, Wiley, 2002.
[23] Kythe P K, *Fundamental solutions for differential operators and applications*, Birkhäuser Boston, 1996.
[24] Partridge P W, Brebbia C A and Wrobel L C, *The Dual Reciprocity Boundary Element Method Computational Mechanics Publications and Elsevier Applied Science*, 1992.
[25] Renardy M and Rogers R C, *An introduction to differential equations*, Springer-Verlag, 1993.
[26] Davies A J, Crann D, Lai C-H and Leong S H, "Time domain decomposition for European options in financial modeling", *Contemporary Mathematics*, Vol. 218, 1998, 486-491.
[27] Davies A J, Honnor M E, Lai C-H, Parrott A K and Rout S, "A distributed Laplace transform method for European options", *Computational Finance and it Applications*, 2004, 157-166.
[28] Davies A J and Lai C-H, "On a distributed algorithm for the solution of nonlinear transient parabolic problems", *DCABES2004*, Vol. 1, 2004, 298-300.
[29] Ingber M S and Davies A J, "High Performance Computing - Special Issue", *Engng. Anal. with Boundary Elements*, Vol. 19, 1997.
[30] Popov V and Power H, "An O(*N*) Taylor series multipole boundary element method for three-dimensional elasticity problems", *Engng. Anal. with Boundary Elements*, Vol. 25, 2001, 7-18.
[31] Davies A J and Crann D, "Parallel Laplace transform methods for boundary element solutions of diffusion-type problems", *Advances in Boundary Element Techniques II*, eds. Denda M, Aliabadi M H and Charafi A, 183-190,Hoggar, 2001.
[32] Davies A J, Crann D and Mushtaq J, "A parallel Laplace transform method for diffusion problems with discontinuous boundary conditions", *Applications of High Performance Computing in Engineering VI*, eds. Ingber M, Power H and Brebbia C A, 3-10, WIT Press, 2000.
[33] Crann D and Davies A J, "The Laplace transform boundary element method for diffusion problems with discontinuous boundary conditions", *Advances in Boundary Element Techniques V*, 2004, 249-254.
[34] Crann D and Davies A J, "The Laplace transform boundary element method for diffusion problems with periodic boundary conditions", *Boundary Elements XXVI*, 2004, 393-402.
[35] Davies A J and Honnor M E, "The Laplace transform dual reciprocity method for nonlinear transient field problems", *BEMXXIV*, 363-372, WIT Press, 2002.
[36] Davies A J and Honnor M E, "Time-domain Laplace transform boundary element methods for diffusion problems", *Aplications of high Performing Computing in Engineering VII*, 65-74, WIT Press, 2002.
[37] Crank J and Phahle R D, "Melting ice by the isotherm migration method", *Bull. Inst. Math. Appl*., Vol. 9, 1973, 12-14.
[38] "Radford L E A Laplace transform solution approach for the isotherm migration method", *PhD thesis*, University of Hertfordshire, UK – to appear 2007.
[39] Davies A J and Crann D, "A Laplace transform solution of the biharnomic diffusion equation", *Boundary Elements XXVIII*, 2006, 243-252.
[40] Davies A J, Crann D and Christianson D B, "The

Laplace transform dual reciprocity boundary element method for electromagnetic heating problems", *Advances in Boundary Element Techniques VI*, 2005, 229-234.

[41] Davies A J, Crann D, Kane S J and Lai C-H, "A Hybrid Laplace transform/finite difference boundary element method for diffusion problems", *Computer Modelling in Engineering and Science*, Vol. 18, 2007, 79-85.

[42] Davies A J, Crann D, Kane S J and Lai C-H, "A time-domain decomposition method for the parallel boundary element solution of diffusion problems", Advances in Boundary Element Techniques VIII – to appear 2007.

Alan Davies is Professor of Mathematics at the University of Hertfordshire. He graduated in mathematics from the University of Southampton in 1968 and obtained an MSc in aeronautical structures and PhD in numerical computation from Imperial College, London. He has worked as a research engineer in the aircraft industry and as an engineer in the food processing industry. Since 1969 he has been employed as a lecturer in mathematics at the University of Hertfordshire, formerly Hatfield Polytechnic, being Head of the Mathematics Department from 1992-2006. He has published more than 100 journal and conference papers and is the author of seven textbooks.

Diane Crann is a graduate in mathematics from the Open University and obtained a PhD in mathematics from the University of Hertfordshire in 2005. Amongst other activities she works as the Mathematics Masterclass organiser at the Royal Institution of Great Britain in London. At the University of Hertfordshire she acts as outreach organiser for the School of Physics, Astronomy and Mathematics. Her research interests in Laplace transforms and boundary element methods have resulted in about thirty journal and conference papers.

On Transformation Methods and Concurrency In Time Domain Computation

Choihong Lai
Department of Mathematical Sciences, University of Greenwich
London SE10 9LS, UK
Email: C.H.Lai@gre.ac.uk

ABSTRACT

The paper examines various transformation methods and their roles in the parallelization of time integration of an unsteady problem in science and engineering.

Keywords: Non-linear problems, Parallel and Distributed Computing, Time marching

1. INTRODUCTION

Many engineering and applied science problems require the solutions of nonlinear diffusion equations where the nonlinear feature usually comes with the material properties or the conductivity. In the case of unsteady problems a time-marching scheme, usually with time step length restrictions, is employed in any temporal integration procedure. These restrictions are usually due to stability criteria of an explicit scheme or the truncation errors of an implicit scheme in approximating the temporal derivatives. Computing time of such numerical methods inevitably becomes significant. On the other hand fine grain parallelization of time stepping becomes difficult and it is almost impossible to achieve a distributed/parallel algorithm that is able to yield a de-coupling of the original problem. There are also many problems which require solution details not at each time step of the time-marching scheme, but only at a few crucial steps and the steady state. Therefore effort in finding fine details of the solutions using many intermediate time steps is considered being wasted. Such effort becomes significant in the case of nonlinear problems where a linearisation process, which amounts to an inner iterative loop within the time-marching scheme, is required. It would be a significant save in computing time when the linearisation process and the time-marching scheme can both be done in parallel. The main objective of the present work is to remove the time stepping and to combine it with parallel/distributed computers.

2. TRANSFORMATION METHODS

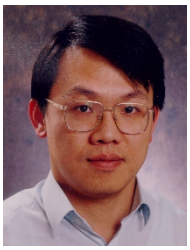
A number of transformation methods and their relations to the possibility of providing concurrency in the solutions of partial differential equations are to be discussed at the presentation. These transformation methods include the Boltzmann transformations, general stretch transformations, Fourier transformation, and Laplace transformation. Several examples related to these transformations are discussed, including diffusion-convection and image processing problems.

The idea of using a Laplace transform is further explored in the context of its numerical inverse for nonlinear problems in flow through porous media [1] and financial computing [2]. This paper examines the idea as a time-domain parallel algorithm suitable for nonlinear parabolic partial differential equations. It involves two levels of temporal mesh. First the numerical solutions of a nonlinear time dependent parabolic problems, using the concept of a Laplace transform and its numerical inverse, are obtained on a coarser temporal mesh. This is essentially an application of the work proposed in [2]. The Laplace transform is applied to a linearisation of the time dependent non-linear parabolic equation leading to a distributed algorithm of solving the resulting set of linear differential equations in the Laplace space. Solutions of the non-linear parabolic equation are then retrieved by means of an approximate inverse Laplace method. A time dependent non-linear parabolic problem is used to illustrate and compare the inverse Laplace method and a temporal integration method. The novel two-level time-domain is then introduced by combining the use of the inverse Laplace method and a temporal integration method. Numerical experiments are provided to examine the efficiency and accuracy of the new algorithm. Finally, discussions and conclusions are presented.

REFERENCES

[1] Moridis G.J. and Reddell D.L., The Laplace transform finite difference method for simulation of flow through porous media, *Water Resources Research*, **27**, pp. 1991, 1873-1884.

[2] Lai C.-H., Parrott A. K., Rout S., A distributed algorithm for European options with nonlinear volatility, Computers and Mathematics with Applications, vol 49, pp. 885~894, 2005.



Choi-Hong Lai is Professor of Numerical Mathematics and head of Scientific Computing and Algorithms Group, School of Computing and Mathematical Sciences, University of Greenwich, UK. His research interest is parallel numerical methods for partial differential equations and their applications in science and engineering. He is the editor of the Journal of Algorithms and Computational Technology, Multi-Science Publishing, UK, the dedicated journal for DCABES post-conference publication, and has edited many special issues for various international journals. He is a Visiting Professor at Southern Yangtze University and an Adjunct Professor at Fuzhou University.

Scalable Parallel Algorithms for Multi-component Problems*

Xiaochuan Cai
Department of Computer Science University of Colorado at Boulder
Boulder, CO 80309, USA
Email:cai@cs.colorado.edu

ABSTRACT

Scalability is one of the most important issues in parallel computations when the size of the problem is large and when the number of processors is large. Domain decomposition methods are very useful for the partitioning of a large problem into many independent subproblems and for solving the problems on large scale parallel computers. The scalability of the methods are well-studied for scalar elliptic equations. In this work we investigate these methods for solving the coupled nonlinear system of equations arising from the discretization of multiphysics problems.

Keywords: Scalability, Nonlinear System

1. INTRODUCTION

Many nature and physical phenomena can be simulated on computers by solving partial differential equations which describe the interplay of the physical variables such as pressure, velocity, energy, etc. The physical variables are often coupled in the sense that if one of them changes at a given time and a point in space other variables change at the same time. However, due to the limitation of computing resources, the physical variables are often simulated separately using techniques such as operator splitting or separation of variables. Using such splitting techniques, each field variable is solved individually. Subiterations are required between the subsystems. The subsystems are easier to solve than the global coupled system, but the iterations between subsystems are sequential. The focus of this report is to investigate a fully coupled approach without splitting the system into subsystems. Such an approach is more parallel than the splitting method, but imposes a lot more pressure on the linear and nonlinear solution methods. We will show that with a powerful domain decomposition based preconditioner the convergence of the iterative methods can be obtained even for some difficult cases. We will report the performance of the algorithms for solving three classes of rather difficult problems.

As the first example, we study the two-dimensional steady-state incompressible Navier-Stokes equations in the primitive variable form [10]:

$$\begin{cases} u \cdot \nabla u - 2\nu \nabla \cdot \varepsilon(u) + \nabla p = f \quad \text{in } \Omega, \\ \nabla \cdot u = 0 \quad \text{in } \Omega, \end{cases} \tag{1}$$

Where $u = (u_1, u_2)^T$ is the velocity, p is the pressure, ν is the dynamic viscosity, and

$$\varepsilon(u) = \frac{1}{2}\left[(\nabla u) + (\nabla u)^T\right]$$

is the symmetric part of the velocity gradient.

One of the popularly used techniques is the projection method which solves the pressure equation and velocity equation separately. In our approach, the two variables p and u stay together throughout the entire computations [3, 13, 14].

As the second example, we consider the numerical simulation of a magnetic reconnection problem described by a system of resistive Hall magnetohydrodynamics equations. The system of equations we model can be derived starting from the momentum transfer equations. Following [1, 12, 18], we can write

$$nm_e\left(\frac{\partial \mathrm{V}_e}{\partial t} + (\mathrm{V}_e \cdot \nabla)\mathrm{V}_e\right) = \tag{2}$$
$$-\nabla p_e - ne(\mathrm{E} + \mathrm{V}_e \times \mathrm{B}) + \nu_e \nabla^2 \mathrm{V}_e + ne\eta \mathrm{j},$$

for the species of electrons and

$$nm_i\left(\frac{\partial \mathrm{V}_i}{\partial t} + (\mathrm{V}_i \cdot \nabla)\mathrm{V}_i\right) = \tag{3}$$
$$-\nabla p_i + ne(\mathrm{E} + \mathrm{V}_i \times \mathrm{B}) + \nu_i \nabla^2 \mathrm{V}_i - ne\eta \mathrm{j},$$

for the species of ions. In (2) and (3) the plasma is considered to be quasi neutral, ions are singly charged, ion/electron number density is n, the resistivity is η, the ion/electron viscosity is given by $\nu_{i,e}$, E is the electric field strength, B is the magnetic induction, j is the current density, $m_{i,e}$ is the ion/electron mass, $V_{i,e}$ is the ion/electron velocity, and $p_{i,e}$ is the ion/electron pressure. Additionally, we introduce

$$ne(\mathrm{V}_i - \mathrm{V}_e) \equiv \mathrm{j}. \tag{4}$$

Maxwell's equations enter the picture via the following three equations:

$$\nabla \cdot B = 0, \tag{5}$$
$$\nabla \times B = \mu_0 j, \tag{6}$$
$$\nabla \times E = -\frac{\partial B}{\partial t}. \tag{7}$$

(2) – (7) provide a full description of the plasma, given certain assumptions on $p_{i,e}$. The incompressibility condition

$$\nabla \cdot V_{i,e} = 0 \tag{8}$$

is added if the plasma is considered incompressible.

As the third example, we consider an inverse elliptic problem [4, 16]: Find the coefficient function $\rho(x)$ in the system

$$\begin{cases} -\nabla \cdot (\rho \nabla u) = f, x \in \Omega \\ u(x) = 0, x \in \partial\Omega. \end{cases} \tag{9}$$

A widely used approach for solving the inverse problem is the output least-squares Tikhonov regularization method, which formulates the ill-posed inverse problem into different stabilized optimization problems, depending on the type of data available [7, 15, 16]. For example, when the measurement of $u(x)$ is given, denoted as $z(x)$, the inverse problem can be transformed into the minimization problem:

$$\text{minimaize } J(\rho, u) = \frac{1}{2}\int_\Omega (u - z)^2 dx + \frac{\beta}{2}\int_\Omega |\nabla \rho|^2 dx, \tag{10}$$

which is often referred to as the "L^2 least-squares problem" which is subject to the constraint (9) satisfied by the

*This work was partially supported by DOE DE-FC02-01ER25479, NSF ACI-0305666, ACI-0352334, and CCF0634594.

pair (ρ, u), and the β-term is called the regularization term. The constant β is the regularization parameter. Instead of solving the constraint optimization problems (10), we turn to solving the saddle-point problem associated with the Lagrangian functional L:

$$L(\rho, u, \lambda) = \frac{1}{2}\int_\Omega (u - z)^2 dx - \int_\Omega (\nabla \cdot \rho \nabla u + f)\lambda dx + \frac{\beta}{2}\int_\Omega |\nabla \rho|^2 dx \quad (11)$$

Hence the solution to the minimization problem can be obtained by solving the corresponding optimality systems: Find (ρ, u, λ) such that

$$\begin{cases} -\beta\Delta\rho + \nabla u \cdot \nabla\lambda = 0 \\ -\nabla\cdot(\rho\nabla\lambda) + (u - z) = 0 \\ -\nabla\cdot(\rho\nabla u) - f = 0. \end{cases} \quad (12)$$

With a finite difference discretization for the steady state problems or an implicit finite difference for the unsteady problem, we obtain a large sparse system of nonlinear equations

$$F(u) = 0,$$

which we will solve using inexact Newton's method:

$$U_{k+1} = U_K - \lambda_k K(U_k)^{-1} F(U_k), k = 0, 1, \ldots \quad (13)$$

Where U_0 is an initial approximation to the solution, $K(U_k) = F'(U_k)$ is the Jacobian at U_k, and λ_K is the steplength determined by a linesearch procedure [8,11]. The inexactness of Newton's method is reflected in the fact that we do not solve the Jacobian systems exactly. The accuracy of the Jacobian solver is determined by some $\eta_K \in [0, 1)$ and the condition

$$\|F(U_k) + K(U_k)s_k\| \le \eta_k \|F(U_k)\|. \quad (14)$$

We use a right-preconditioned GMRES to solve the linear system [20]; i.e., the vector S_k is obtained by approximately solving the linear system $K(E_k)B_k^{-1}(B_k s_k) = -F(E_k)$, where B_k^{-1} is an overlapping Schwarz preconditioner to be discussed in the next section.

2. OVERLAPPING DOMAIN DECOMPOSITION METHODS

We briefly introduce the multilevel Schwarz preconditioner [19, 21,22]. The multilevel preconditioner is applicable to general linear systems arising from the discretized PDEs on a mesh using finite element or finite difference methods. Let $\Omega \subset R^2$ be a bounded open domain on which a PDE is defined and a discretization is performed with a mesh Ω_h of characteristic size $h > 0$. To obtain the overlapping partition, we first divide Ω_h into non-overlapping subdomains Ωj, $j = 1, \ldots, N_S$. We then expand each Ωj to $\Omega j'$, i.e., $\Omega j \subset \Omega_j'$. The overlap $\delta > 0$ is defined as the minimum distance between $\partial\Omega_j'$ and $\partial\Omega_j$, in the interior of Ω. For boundary subdomains we simply cut off the part outside Ω. Let $H > 0$ denote the characteristic diameter of $\{\Omega j\}$.

Let N and N_j denote the number of degrees of freedom associated to Ω and Ω_j', respectively. Let N be a $N \times N$ sparse matrix of a linear system

$$K_P = b \quad (15)$$

generated during the Newton iterations. Let d be the degree of freedom per mesh point. For simplicity let us assume that d is the same throughout the entire mesh. We define the $N_j \times N$ matrix R_j^δ as follows: its $d \times d$ block element $(R_j^\delta)_{l_1,l_2}$ is either (a) an identity block if the integer indices $1 \le l_1 \le N_j/d$ and $1 \le l_2 \le N/d$ are related to the same mesh point and this mesh point belongs to Ω_j' or (b) a zero block otherwise. The multiplication of R_j^δ with a $N \times 1$ vector generates a smaller $N_j \times 1$ vector by discarding all components corresponding to mesh points outside Ω_j'. Let $\tilde{K}_j$ be defined as

$$\tilde{K}_j \equiv R_j^\delta K (R_j^\delta)^T,$$

that is, as the $N_j \times N_j$ matrix related to a subdomain problem having zero Dirichlet boundary conditions at regions of $\partial\Omega_j'$ not coinciding with $\partial\Omega$. We assume $\tilde{K}_j$ to be nonsingular and denote by $\tilde{B}_j^{-1}$ either the inverse of or a preconditioner for $\tilde{K}_j$. The one-level classical additive Schwarz preconditioners for K is defined as [9]

$$B_{\delta\delta}^{-1} = \sum_{j=1}^{Ns} (R_j^\delta)^T \tilde{B}_j^{-1} R_j^\delta.$$

For the description of multilevel Schwarz preconditioners [23], let us use index i = 0, 1, . . . ,L−1 to designate any of the $L \ge 2$ levels. All previously defined entities using the subindex "j" will now use double subindexes "i, j": $\Omega_{i,j}$, $\Omega_{i,j}'$, $N_{i,j}$, $R_{i,j}^\delta$, $\tilde{K}_{i,j}$ and $\tilde{B}_{i,j}^{-1}$. All previously defined entities using no subindex will now use the subindex "i": $h_i, N_i, N_{s,i}, H_i, \delta_i, B_{i,\delta\delta}^{-1}, B_i^{-1}$, and K_i, with the eventual notation $K_{L-1} = K$. The L meshes are not assumed to be either nested or structured. Let I_i denote the identity operator and, for $i > 0$, let

$$I_i^{i-1} : R^{N_i} \to R^{N_{i-1}}$$

denote a linear restriction operator from level i to level $i-1$ and let

$$I_{i-1}^{i} : R^{N_{i-1}} \to R^{N_i}$$

denote a linear interpolation operator from level $i-1$ to level i. Given the iterate used for the computation of K_{L-1}, the computation of coarse matrices K_i (i.e., $0 \le i \le L-2$) proceeds recursively from the finest coarse level $i = L-2$ until the coarsest level $i = 0$ by simply first restricting or injecting the finer iterate and then computing the Jacobian. Multilevel Schwarz preconditioners are obtained through the combination of one-level Schwarz preconditioners B_i^{-1} assigned to each level. Here we focus on multilevel preconditioners that can be seen as multigrid (MG) V-cycle algorithms [2] having Schwarz preconditioned Richardson working as the pre and the post smoother at each level $i > 0$, with $B_{i,pre}^{-1}$,pre preconditioning the $\mu_i \ge 0$ pre smoother iterations and $B_{i,post}^{-1}$,post preconditioning the $\nu_i \ge 0$ post smoother iterations. In a general MG V-cycle algorithm with

$L \geq 2$ levels, given the current iterate $p^{(\ell)}$ for the solution of (15), the next iterate is computed as $p^{(\ell+1)} = A\lg V\left(b, L, p^{(\ell)}\right)$, where the procedure $v_i = A\lg V\left(b_i, i, v_i\right)$ consists of the following steps:

if $i = 0$
  Solve $K_0 v_0 = b_0$;
else
  Smooth u_i times $K_i v_i = b_i$;
  $b_{i-1} = I_i^{i-1}\left(b_i - K_i v_i\right)$;
  $v_{i-1} = A\lg V\left(b_{i-1}, i-1, 0\right)$;
  $v_i = v_i + I_{i-1}^{i} v_{i-1}$;
  Smooth v_i times $K_i v_i = b_i$;
end

In this report we consider multilevel Schwarz preconditioners with coarsest correction computed as

$$v_0 = B_0^{-1} b_0,$$

where B_0^{-1} might denote either a Schwarz preconditioner or an exact solver.

When classic Schwarz preconditioners are applied to symmetric positive definite systems arising from the discretization of elliptical problems defined in $H_0^1(\Omega)$, the condition number κ of the preconditioned system satisfies $\kappa \leq C\left(1 + H/\delta\right)/H^2$ for one-level methods and $\kappa \leq C\left(1 + H/\delta\right)$ for two-level methods, where C is independent of *h*, *H* and δ. The factor $1/H^2$, associated to the number of subdomains on the fine level, relates itself to the increase on the number of iterations (needed for the exchange of information among distant subdomains) with the increase in the total number of subdomains. The use of a coarse level helps the exchange of information. The necessity of information exchange among distant domain regions can be understood through the expression of the solutions of elliptic problems in terms of Green's functions: although the solution value at a point strongly depends on surrounding values, there is weaker dependence w.r.t. the entire domain [21]. Regarding the application of two-level methods to indefinite model problems, the study in [5] suggests that the coarse mesh needs to be sufficiently fine for the multilevel Schwarz preconditioner to perform well.

Theoretically, however, these results may not be directly applied to systems of PDEs that are not elliptic. This includes the cases mentioned in Section 1. Let l be the average number of linear iterations per Newton step. We then look for the following scalability properties when applying a multilevel preconditioner:

- The processor scalability: For fixed h and H/δ, is not very sensitive to H decreasing,
- The mesh size scalability: For fixed H and δ, l is not very sensitive to the mesh refinement.

REFERENCES

[1] S. I. Braginskii, *Reviews of Plasma Physics*,Vol 1, Consultants Bureau, New York, 1965.

[2] W. L. Briggs, V. E. Henson, and S. F. Mc-Cormick, *A Multigrid Tutorial*, SIAM, Second ed., 2000.

[3] X.-C. Cai and D. E. Keyes, *Nonlinearly preconditioned inexact Newton algorithms*, SIAM J. Sci. Comput., 24 (2002) 183–200.

[4] X.-C. Cai, S. Liu, and J. Zou, *An overlapping domain decomposition method for parameter identification problems*, Lecture Notes in Computational Science and Engineering, Springer, (2007), to appear.

[5] X.-C. Cai and O. B. Widlund, *Domain decomposition algorithms for indefinite elliptic problems*, SIAM J. Sci. Statist. Comput., 13 (1992), pp. 243–258.

[6] Z. M. Chen and J. Zou, *Finite element emethods and their convergence for elliptic and parabolic interface problems*, Numer. Math., 79 (1998), pp. 175-202.

[7] Z. M. Chen and J. Zou, *An augmented Lagrangian method for identifying discontinuous parameters in elliptic systems*, SIAM J. Control Optim., 37 (1999), 892-910.

[8] J. Dennis and R. B. Schnabel, *Numerical Methods for Unconstrained Optimization and Nonlinear Equations*, SIAM, Philadelphia, 1996.

[9] M. Dryja and O. Widlund, *Domain decomposition algorithms with small overlap*, SIAM J. Sci. Comp., 15 (1994), pp. 604–620.

[10] M. D. Gunzburger, *Finite Element Methods for Viscous Incompressible Flows*, Academics Press, New York, 1989.

[11] S. Eisenstat and H. Walker, *Globally convergent inexact Newton methods*, SIAM J. Optim.,4 (1994), pp. 393–422.

[12] R. Fitzpatrick, *Scaling of forced magnetic reconnection in the Hall-magnetohydrodynamic Taylor problem*, Phys. Plasmas, 11 (2004), 937–946.

[13] F.-N. Hwang and X.-C. Cai, *A parallel nonlinear additive Schwarz preconditioned inexact Newton algorithm for incompressible NavierStokes equations*, J. Comput. Phys., 204(2005), 666-691.

[14] F.-N. Hwang and X.-C. Cai, *Parallel fully coupled Schwarz preconditioners for saddle point problems*, ETNA, 22 (2006), pp. 146-162.

[15] K. It^o and K. Kunish, *The augmented Lagrangian method for parameter estimation in elliptic systems*, SIAM J. Control Optim., 28(1990), pp. 113-136.

[16] Y. L. Keung and J. Zou, *An efficient linear solver for nonlinear parameter identification problems*, SIAM J. Sci. Comput., 22 (2001), pp. 1511-1526.

[17] A. Kirsch, *An Introduction to the MathematicalTheory of Inverse Problems*, Springer-Verlag, 1996.

[18] S. Ovtchinnikov, F. Dobrian, X.-C. Cai, and D. Keyes, *Additive Schwarz-based fully coupled implicit methods for resistive Hall magnetohydrodynamic problems*, J. Comput. Phys., (2007), to appear.

[19] E. Prudencio and X.-C. Cai, *Parallel multilevel restricted Schwarz preconditioners with pollution removing for PDE-constrained optimization*, SIAM J. Sci. Comput., 29 (2007), pp.964-985.

[20] Y. Saad, *Iterative Methods for Sparse Linear Systems*, SIAM, Philadelphia, 2003.

[21] B. Smith, P. Bjørstad, and W. Gropp, *Domain Decomposition: Parallel Multilevel Methods for Elliptic Partial Differential Equations*, Cambridge University Press, Cambridge, MA, 1996.

[22] A. Toselli and O. Widlund, *Domain Decomposition Methods – Algorithms and Theory*, Springer-Verlag, 2005.

[23] X. Zhang, *Multilevel Schwarz methods*, Numer. Math., 63 (1992), pp. 521–539.

A Parallel Block SPP Solver for Multidimensional Tridiagonal Equations With Optimal Message Vector Length*

H. Guo[1], Z. Yin[2], L.Yuan[1]
[1]LSEC and Institute of Computational Mathematics and Scientific/Engineering Computing
Academy of Mathematics & Systems Science
[2]National Microgravity Laboratory, Institute of Mechanics
Chinese Academy of Sciences, Beijing, 100080, P.R.China
Email: [1]Zhaohua.yin@imech.ac.cn , [2]Guoh@lsec.cc.ac.cn

ABSTRACT

The parallel strategy of solving multidimensional tridiagonal equations is investigated in this paper. We present detailed implementation of an improved version of single parallel partition (SPP) algorithm in conjunction with message vectorization, which aggregates several communication messages into one to reduce the communication costs. We show the improved SPP can achieve very good speedup for a wide range of message vector length (MVL), especially for the problems when the number of grid points on divided direction is large. Instead of only using the largest possible MVL, we adopt numerical tests and modeling analysis to determine an optimal MVL, and even better speedup is achieved.

Keywords: Tridiagonal Equation, Single Parallel Partition, Message Vectorization, Message Vector Length

1. INTRODUCTION

The tridiagonal system plays an important role in computational sciences. A large number of direct parallel algorithms for solving a tridiagonal system of equations were developed in the past four decades, e.g. the transpose strategy [1], the pipelined method [2], and the message vectorization [3].

In terms of generality and simplicity, the so-called P-scheme is very attractive for solving a very large system on a parallel computer [4]. However, it requires large data transport, which takes too much time in communication. Later on a modification from Wang's partition method [5], named Single Parallel Partition algorithm (SPP), was introduced in [6]. This algorithm leads to a big reduction in data transport, without any significant increase of the number of operation for executing the complete algorithm. However, it could not achieve satisfying speedup compared with the pursuit method on a single processor. This is because the computational counts of SPP are far more than those of pursuit method.

When many unrelated (or, multidimensional) tridiagonal equations are considered, the shortcoming of SPP mentioned above can be overcome with the idea of message vectorization adopted, which aggregates data sending instead of "one by one" sending. Wakatani combined message vectorization with his new parallel tridiagonal solver, the P-scheme [3], to solve two-dimensional ADI equations with a wide range of problem sizes, and the super-linear speedup was observed when the size of the problem was 16386×16386.

Although message vectorization has proved useful when applied to P-scheme, there is still no effort so far to combine it with SPP scheme. In this paper, we applied SPP in conjunction with message vectorization. Section 2 briefly describes the original SPP algorithm, and its computational complexity is also presented. Section 3 first provides the implementation of SPP with message vectorization, and then presents the description of the improved SPP algorithm. In the later part of section 3, we analyze the parallel efficiency of the improved SPP and its performance on local parallel computers. We have found that the best speedup does not correspond to the maximum MVL, and the improved SPP is more suitable for the problems when the number of grid points on divided direction is larger than that of other directions. Conclusions are given finally.

* This project is supported by NSF of China (G10502054, G10432060) and CAS Innovation Program. LY is supported by NSF of China (G10476032, G1053108)

2. THE ORIGINAL SPP ALGORITHM

2.1 A Brief Description of SPP

We considere the tridiagonal system of equations of order n:

$$Ax=\begin{pmatrix} d_1 & c_1 & & & \\ a_2 & d_2 & c_2 & & \\ & \ddots & \ddots & \ddots & \\ & & a_{n-1} & d_{n-1} & c_{n-1} \\ & & & a_n & d_n \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix}=\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ b_n \end{pmatrix}=b, \qquad (1)$$

and we consider the situation when there is a unique solution x existing for given right-hand side b and nonsingular coefficient matrix A. The matrix A is subdivided in p (the number of processors available) groups of k rows, and we assume $n=p*k$. All processors have a local memory and the data have been spread over the local memories. The local memory of each processor contains only the matrix- and vector-elements of the k rows of the ith group.

SPP algorithm can be described as follows:

1. Each processor (denote as N_0 , N_1 , … , N_{p-1}) reads its own data.
2. For N_i, i=0,⋯, p-2, reduce d_{ik+1} to 1, then eliminate a_{ik+2}, then reduce d_{ik+2} to 1, and go on until a_i, i=2,⋯, n-k are all eliminated;
3. For N_i, i=1,⋯, p-1, reduce d_{ik+k} to 1, then eliminate c_{ik+k-1}, then reduce d_{ik+k-1} to 1, and go on until c_i, i=k+1,⋯, n are all eliminated.
4. For N_{p-1}, send $a_{(p-1)k+1}$ and $b_{(p-1)k+1}$ to N_{p-2}. For N_i, i=p-2,⋯,1, receive elements sent from N_{i+1}, eliminate $a_{(i+1)k+1}$ on N_i, reduce the resulting $d_{(i+1)k+1}$ to 1 using the elements of (i+1)kth line, and then eliminate c_{ik+1} on the first line. Send the new a_{ik+1} and b_{ik+1} to N_{i-1}.
5. For N_0, once receiving element a_{k+1} sent from N_1, eliminate a_{k+1} on N_0, and then reduce $d_{(i+1)k+1}$ to 1 and eliminate c_k. After the communication of data, eliminate

c_i left on $N_1,\cdots, N_{p-2}$.

6. For N_0, send b_k to N_1. For N_i, $i=1,\cdots, p-2$, receive elements sent from N_{i-1}, $a_{(i+1)k}$, and then send $b_{(i+1)k}$ to N_{i+1}. For N_{p-1}, receive elements sent from N_{p-2}, and then eliminate $a_{(p-1)k+1}$.
7. When communications are completed, eliminate the nondiagonal elements remained on each processor. b_i, $i=1,\cdots, n$, are the answers to Eq.(1).

The 2) and 3) parts of the scheme can be readily parallelized.

2.2 Computation and Communication Counts

The total time (T_{sum}) for each processor can be expressed as following:

$$T_{sum} = T_{comp} + T_{comm} = T_{comp} + T_{sendrecv} + T_{delay}, \quad (2)$$

where T_{comp} is the sum of the computation time and T_{comm} the communication time. T_{comm} can be divided into two parts: transmission time ($T_{sendrecv}$) and latency time (T_{delay}) (e.g., see [7]). From [6], we can get the total time on multiprocessors for SPP

$$T_{spp} = \left(12\frac{n}{p} - 14\frac{n}{p^2}\right)t_c + 6(p-1)t_{sendrecv} + 4(p-1)t_{delay} \quad p>1. \quad (3)$$

Here, t_c is the per-element computational time in a single processor, $t_{sendrecv}$ the time to transmit an element between processors, and t_{delay} the latency time for a message passing.

It should be noticed that the total time for the classic pursuit method on one computer is

$$T_{purs} = 5nt_c. \quad (4)$$

It is clear that although the operation counts in SPP are smaller compared with other algorithms such as the P-scheme[3], they are still larger than those in pursuit method. It is hard to reduce the computation time of SPP, so the only way to make SPP efficient is to lower the communication costs.

3. THE BLOCK SPP ALGORITHM

In this section, we will try to use modeling analysis and real application on supercomputers to reduce T_{comm} on multidimensional system. Since the total data to be transferred in SPP is very few, $T_{sendrecv}$ is expected to be very low and T_{delay} should be reduced to make SPP efficient.

3.1 Message Vectorization

For multidimensional system, SPP can be applied aggregately to several data instead of the "one by one" approach. Several data sent in one time can reduce the frequency for message passing, and the latency cost can be reduced dramatically. By aggregating m data into one message, the communication cost for m data is reduced to $t_{delay}+mt_{sendrecv}$ instead of $m(t_{delay}+t_{sendrecv})$ [3]. In this paper, we denote SPP with message vectorization as *the block SPP algorithm*.

Without losing the generality, we assume that only one dimension of arrays is distributed among processors, and the SPP scheme can be implemented in the divided dimension. We adopt the general used three dimensional cases as the example, and (i_{dm}, j_{dm}, k_{dm}) denote the number of points in x, y and z coordinate directions, respectively. If x direction of the grid is divided across the number of processors, the size of message transmitted from one processor to another in one communication (MVL) can be from 1 to $j_{dm}\times k_{dm}$.

3.2 Description of Block SPP

In the following description of program structure of block SPP, we assume that the size of the MVL is m and the x direction of the grid is evenly divided by p processors:

If $1 \leqslant m \leqslant j_{dm}$, the processing of block SPP involved is given by:

for $K=1,\cdots,k_{dm}$ *do*
for $L=1,\cdots,j_{dm}/m$ *do*
for $J=m(L-1)+1,\cdots,mL$ *do*
{{{

$$g_{ik+1,J,K} \leftarrow \frac{c_{ik+1,J,K}}{d_{ik+1,J,K}}, \qquad i=0,\cdots,p-2$$

$$b_{ik+1,J,K} \leftarrow \frac{b_{ik+1,J,K}}{d_{ik+1,J,K}}, \qquad i=0,\cdots,p-2$$

$$f_{ik+1,J,K} \leftarrow \frac{a_{ik+1,J,K}}{d_{ik+1,J,K}}, \qquad i=1,\cdots,p-2$$

for $j=2,\cdots,k$ *do*
{

$$df_{ik+j,J,K} \leftarrow d_{ik+j,J,K} - g_{ik+j-1,J,K}\times a_{ik+j,J,K}, \quad i=0,\cdots,p-2$$

$$g_{ik+j,J,K} \leftarrow \frac{c_{ik+j,J,K}}{df_{ik+j,J,K}}, \qquad i=0,\cdots,p-2$$

$$b_{ik+j,J,K} \leftarrow \frac{b_{ik+j,J,K} - b_{ik+j-1,J,K}\times a_{ik+j,J,K}}{df_{ik+j,J,K}}, \quad i=0,\cdots,p-2$$

$$f_{ik+j,J,K} \leftarrow \frac{-f_{ik+j-1,J,K}\times a_{ik+j,J,K}}{df_{ik+j,J,K}}, \qquad i=1,\cdots,p-2$$

}

$$f_{ik+k,J,K} \leftarrow \frac{a_{ik+k,J,K}}{d_{ik+k,J,K}}, \qquad i=p-1$$

$$f_{ik+k,J,K} \leftarrow \frac{f_{ik+k,J,K}}{d_{ik+k,J,K}}, \qquad i=1,\cdots,p-2$$

$$b_{ik+k,J,K} \leftarrow \frac{b_{ik+k,J,K}}{d_{ik+k,J,K}}, \qquad i=1,\cdots,p-1$$

$$g_{ik+k,J,K} \leftarrow \frac{g_{ik+k,J,K}}{d_{ik+k,J,K}}, \qquad i=1,\cdots,p-2$$

for $j=k-1,\cdots,1$ *do*
{

$$df_{ik+j,J,K} \leftarrow d_{ik+j,J,K} - c_{ik+j,J,K}\times f_{ik+j+1,J,K}, \quad i=p-1$$

$$f_{ik+j,J,K} \leftarrow \frac{a_{ik+j,J,K}}{df_{ik+j,J,K}}, \qquad i=p-1$$

$$b_{ik+j,J,K} \leftarrow \frac{b_{ik+j,J,K} - b_{ik+j+1,J,K}\times g_{ik+j,J,K}}{df_{ik+j,J,K}}, \quad i=p-1$$

$$f_{ik+j,J,K} \leftarrow f_{ik+j,J,K} - f_{ik+j+1,J,K}\times g_{ik+j,J,K}, \quad i=1,\cdots,p-2$$

$$b_{ik+j,J,K} \leftarrow b_{ik+j,J,K} - b_{ik+j+1,J,K}\times g_{ik+j,J,K}, \quad i=1,\cdots,p-2$$

$$g_{ik+j,J,K} \leftarrow -g_{ik+j,J,K}\times g_{ik+j+1,J,K}, \qquad i=1,\cdots,p-2$$

}}

{

receive $f_{(i+1)k+1,J,K}, b_{(i+1)k+1,J,K}$ from $N_{i+1}, J = m(L-1)+1,\cdots,m$

$i = p-2,\cdots,0$

for $J = m(L-1)+1,\cdots,mL$ do

{

$df_{(i+1)k+1,J,K} \leftarrow 1 - f_{(i+1)k+1,J,K} \times g_{(i+1)k,J,K}$, $i = p-2,\cdots,0$

$b_{(i+1)k+1,J,K} \leftarrow \dfrac{b_{(i+1)k+1,J,K} - b_{(i+1)k,J,K} \times f_{(i+1)k+1,J,K}}{df_{(i+1)k+1,J,K}}$, $i = p-2,\cdots,0$

$f_{(i+1)k+1,J,K} \leftarrow \dfrac{-f_{(i+1)k,J,K} \times f_{(i+1)k+1,J,K}}{df_{(i+1)k+1,J,K}}$, $i = p-2,\cdots,1$

$b_{ik+1,J,K} \leftarrow b_{ik+1,J,K} - b_{(i+1)k+1,J,K} \times g_{ik+1,J,K}$, $i = p-2,\cdots,1$

$f_{ik+1,J,K} \leftarrow f_{ik+1,J,K} - f_{(i+1)k+1,J,K} \times g_{ik+1,J,K}$, $i = p-2,\cdots,1$

$b_{k,J,K} \leftarrow b_{k,J,K} - b_{k+1,J,K} \times g_{k,J,K}$, $i = 0$

}

Send $f_{ik+1,J,K}, b_{ik+1,J,K}$ to $N_{i-1}, J = m(L-1)+1,\cdots,m$

$i = p-1,\cdots,1$

for $J = m(L-1)+1,\cdots,mL$ do

for $j = 2,\cdots,k$ do

{{

$b_{ik+j,J,K} \leftarrow b_{ik+j,J,K} - b_{(i+1)k+j,J,K} \times g_{ik+j,J,K}$, $i = 1,\cdots,p-2$

$f_{ik+j,J,K} \leftarrow f_{ik+j,J,K} - f_{(i+1)k+j,J,K} \times g_{ik+j,J,K}$, $i = 1,\cdots,p-2$

}}}

do the latter from N_0 to N_{p-1} one by one

{

Recv $b_{ik,J,K}$ from $N_{i-1}, J = m(L-1)+1,\cdots,m$, $i = 1,\cdots,p-1$

for $J = m(L-1)+1,\cdots,mL$ do

{

$b_{(i+1)k,J,K} \leftarrow b_{(i+1)k,J,K} - b_{ik,J,K} \times f_{(i+1)k,J,K}$, $i = 1,\cdots,p-2$

}

Send $b_{(i+1)k,J,K}$ to $N_{i+1}, J = m(L-1)+1,\cdots,m$, $i = 0,\cdots,p-2$

}

for $J = m(L-1)+1,\cdots,mL$ do

for $j = 1,\cdots,k-1$ do

{{

$b_{ik+j,J,K} \leftarrow b_{ik+j,J,K} - b_{(i+1)k+j,J,K} \times f_{ik+j,J,K}$, $i = 1,\cdots,p-2$

}}

for $J = m(L-1)+1,\cdots,mL$ do

for $j = 1,\cdots,k$ do

{{

$b_{ik+j,J,K} \leftarrow b_{ik+j,J,K} - b_{ik+j-1,J,K} \times f_{ik+j,J,K}$, $i = p-1$

}}

}}

When $j_{dm} < m \leqslant j_{dm} \times k_{dm}$, the procedure is all the same except changing the circulation from

$K = 1,\cdots,k_{dm}$

$L = 1,\cdots,j_{dm}/m$

$J = m(L-1)+1,\cdots,mL$

to

$L = 1,\cdots,k_{dm} \times j_{dm}/m$

$K = m(L-1)/j_{dm}+1,\cdots,mL/j_{dm}$

$J = 1,\cdots,j_{dm}$

In the following, we will try to follow the structure of the program described above to analyze the parallel character of block SPP. The speedup of a parallel algorithm is affected by many factors, and what we are doing here is to simply employ an approximate parallel model which has been used before in the block pipelined method [2].

The number of iterations for all the message vectors to be sent:

$$l = \frac{j_{dm} \times k_{dm}}{m}. \tag{5}$$

In the data propagation process of the block SPP algorithm, all processors except the first one must wait for the data to be sent by the previous processor, and the time for the last processor to receive the message will be the time for the first processor to begin its pth iteration sending. The job is done until all processors finish their own iterations. Therefore, the whole number of sending iterations throwing off the overlapped ones is $l+p$-1. In general, we can get the total time used for solving all $j_{dm} \times k_{dm}$ scalar tridiagonal matrix equations in the x direction:

$$\begin{aligned} T_{sum} &= (l+p-1)\left[6\frac{j_{dm}k_{dm}}{l}t_{sendrecv} + 4t_{delay} + 8\frac{i_{dm}j_{dm}k_{dm}}{l}\varepsilon t_c\right] \\ &\quad + l\left[\frac{i_{dm}j_{dm}k_{dm}}{l}\left(\frac{12}{p} - \frac{14}{p^2} - 8\right)\varepsilon t_c\right] \\ &= a/l + b \cdot l + c, \end{aligned} \tag{6}$$

where

$$a = 6\,j_{dm}k_{dm}(p-1)t_{sendrecv} + 8\,i_{dm}\,j_{dm}k_{dm}(p-1)\varepsilon t_c$$

$$b = 4t_{delay}$$

$$c = 6\,j_{dm}k_{dm}t_{sendrecv} + 4(p-1)t_{delay} + i_{dm}\,j_{dm}k_{dm}\left(\frac{12}{p} - \frac{14}{p^2}\right)\varepsilon t_c,$$

and $\varepsilon < 1$ is a factor representing the influence of the cache hit rate on computational time. For the time being, we assume ε is constant. Then there is an equilibrium l that makes T_{sum} minimal:

$$l_{opt} = \sqrt{a/b}. \tag{8}$$

Thus we have the optimal message vector length:

$$\begin{aligned} m_{opt} &= j_{dm} \times k_{dm}\sqrt{\frac{b}{a}} \\ &= \sqrt{\frac{2\,j_{dm}k_{dm}t_{delay}}{(3t_{sendrecv} + 4i_{dm}\varepsilon t_c)(p-1)}}. \end{aligned} \tag{9}$$

The idea of message vectorization gives people the feeling that larger MVL will lead to better parallel efficiency. However, this is not always the case since normally we have

$$\frac{2t_{delay}}{(3t_{sendrecv} + 4i_{dm}\varepsilon t_c)(p-1)} < j_{dm}k_{dm},$$

and $1 < m_{opt} < j_{dm} \times k_{dm}$.

Moreover, from Eq. (9), we can easily get the following conclusions:

1. For the fixed p and $j_{dm} \times k_{dm}$, m_{opt} is smaller when i_{dm} is larger.
2. For the fixed $i_{dm} \times j_{dm} \times k_{dm}$, m_{opt} is smaller when p is larger.

3.3 Experiment with the Block SPP and Optimal Message Vector Length

We apply the parallel strategy above with MPI FORTRAN on Lenovo DeepComp 1800 cluster. We measure the wall time for executing only the *x* direction sweep. The speedup factor is the wall clock time of the pursuit method divided by that of the block SPP algorithm in the same resolution. Three different kinds of solutions are used: 64^3, 256×64^2 and 1024×64^2, and the possible values of MVL are from 1 to 4096.

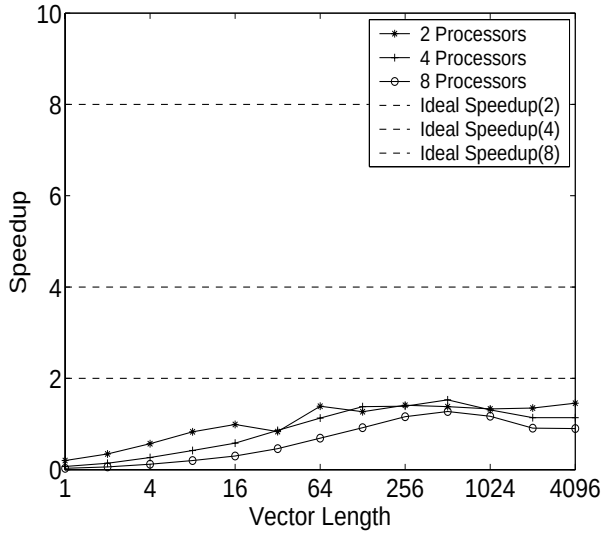


Fig. 1. Speedups of the SPP with message vectorization for an 64^3 problem.

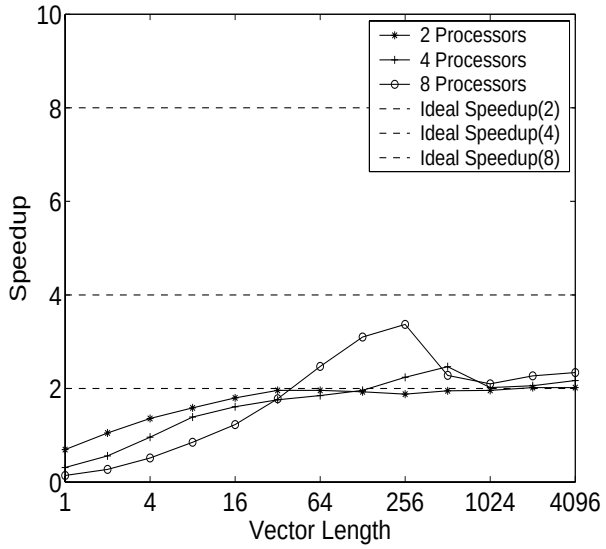


Fig. 2. Speedups of the SPP with message vectorization for a 256×64^2 problem.

Table 1. The values of optimal MVL for different resolutions and processor numbers.

	2 Processors	4 Processors	8 Processors
64×64^2	MVL=4096	MVL=512	MVL=512
256×64^2	MVL=2048	MVL=512	MVL=256
1024×64^2	MVL=2048	MVL=256	MVL=64

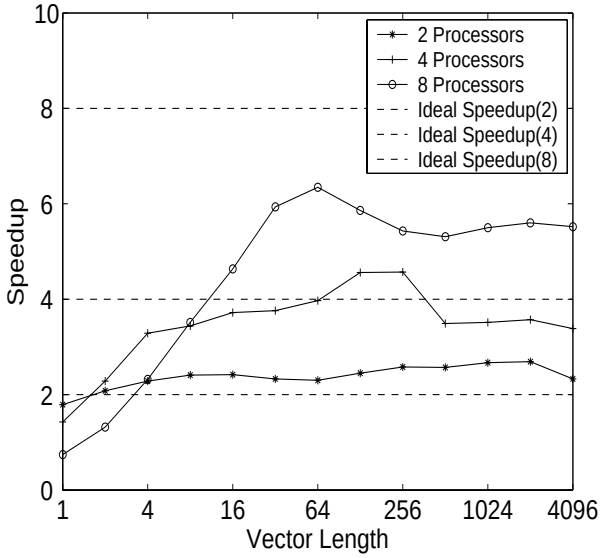


Fig.3. Speedups of the SPP with message vectorization for a 1024×64^2 problem.

From Fig. 1, we can see that although the speedup of the block SPP is better than the original SPP without any message vectorization (or MVL equals to 1), it is far away from the ideal speedup even for the some small-size problems. This is due to larger computational complexities of SPP compared with the pursuit method. For the 256×64^2 problem, the speedup is only slightly better than that in the 64^3 problem (Fig. 2).

The situation is quite different when i_{dm} is larger. For a 1024×64^2 problem (Fig. 3), we see super-linear speedup is achieved for MVL in the range of 2 ~ 4096 on 2 processors and 64 ~ 256 on 4 processors. When the size of array is large, the effect of the computational complexity is counteracted by the improved cache hit rate. Although there is no super-linear speedup achieved on 8 processors, the parallel efficiency of 1024×64^2 is much better than that of the 256×64^2 problem.

As predicted in the previous subsection, the maximum speedup does not always occur at the largest MVL but rather at some intermediate MVL. In the case of the 64^3 problem, the optimal MVL is 4096 only in the case of 2 processors. For 4 or 8 processors, the optimal MVL is 512. In the case of the 256×64^2 and 1024×64^2 problems, the optimal MVL never appears as the largest MVL. Moreover, as predicted by our model, the value of optimal MVL decreases when p becomes larger. In the case of 1024×64^2, the value of optimal MVL will be divided by four when p is doubled each time.

Table 1 shows the relation of p and optimal MVL for three resolutions, and m_{opt} is smaller when i_{dm} is larger for fixed p and $j_{dm}\times k_{dm}$. This also fits the conclusion drawn from Eq. (9). Our analyzing model, although simple, is effective in explaining the parallel character of our simulations.

Fig. 4 shows the optimal speedup of our code vs. different CPU numbers. The values adopted here are the speedup factor when optimal MVL is applied for certain P and resolution. Good parallel efficiency is obtained with the optimal MVL.

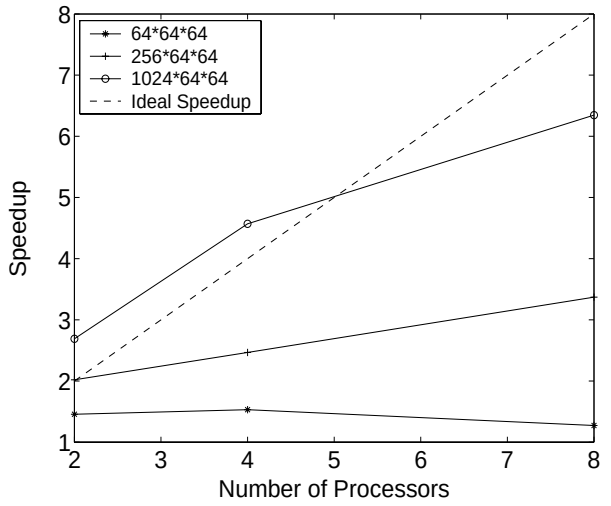


Fig. 4. Optimal Speedups.

4. CONCLUSIONS

In this paper, we have presented an improved version of the SPP algorithm with message vectorization, and demonstrated that good speedup for 3D problems could be got with the improved SPP scheme. Super-linear speedups can be obtained when the number of grids on the divided direction is large enough. We have also developed a simple parallel model which can forecast the existence of the optimal message vector length. The implement of optimal MVL leads to good speedup in our numerical experiment on the supercomputer.

REFERENCES

[1] T.M. Edison, G. Erlebacher, "Implementation of a fully-balanced periodic tridiagonal solver on a parallel distributed memory architecture", *Concurrency-pract EX* 7:4, 1995, pp.273-302.

[2] L.B. Zhang, "On pipelined computation of a set of recurrences on distributed memory systems", *Journal on Numerical Methods and Computational Applications*, Vol.3, 1999, pp.184~191.

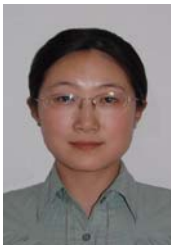
[3] A. Wakatani, "A parallel and scalable algorithm for ADI method with pre-propagation and message vectorization", *Parallel Computing*, Vol.30, 2004, pp.1345~1359.

[4] A. Wakatani, "A parallel scheme for solving a tridiagonal matrix with pre-propagation", in: Proc. 10th *Euro PVM/MPI Conference*, 2003.

[5] H.H. Wang, "A Parallel Method for Tridiagonal Equations", *ACM Transactions on Mathematical Software*, Vol.7, No.2, 1981, pp.170~183.

[6] C.R. Wang, Z.H. Wang, X.H. Yang, *Computational Fluid Dynamics and Parallel Algorithms*, first ed., National University of Defence Technology Press, Changsha, 2000.

[7] Z. Yin. Li Yuan, Tao Tang, "A new parallel strategy for two-dimensional incompressible flow simulations using pseudo-spectral methods", *Journal of Computational Physics*, Vol.210, 2005, pp.325~341.



Hong Guo is a Ph.D student of LSEC and Institute of Computational Mathematics and Scientific/Engineering Computing, Academy of Mathematics & Systems Science, Chinese Academy of Sciences. She graduated from Jilin University in 2001; from Hebei University of Technology in 2004 with specialty of computer graphics. Her Ph.D supervisor was Prof. Li Yuan. Her research interests are in distributed parallel processing and computational fluid dynamics

Zhaohua Yin is an assistant professor in National Microgravity Laboratory, Institute of Mechanics, Chinese Academy of Sciences. He got his Bachelor degree (1991) and Master degree (1999) in Peking University (China), and Ph.D degree (2003) in Technical University of Eindhoven (the Netherlands) under the supervision of Prof. David C. Montgomery. His research interests are parallel computing, direct simulation of turbulence and two-phase microgravity flows.

Yuan Li is a professor in LSEC and Institute of Computational Mathematics and Scientific/Engineering Computing, Academy of Mathematics & Systems Science, Chinese Academy of Sciences. He got his PhD degree in Beijing University of Aeronautics and Astronautics (1992). His research interest is computational study of transitional flows, numerical methods for compressible multicomponent flows and chemically reacting flows.

Towards Parallel Program Verification*

Pei He[1,2], Lishan Kang[1,3]
[1]State Key Laboratory of Software Engineering, Wuhan University
Wuhan, Hubei 430072, P. R. China
[2]School of Computer and Communication Engineering, Changsha University of Science and Technology
Changsha, Hunan 410076, P. R. China
[3]School of Computer, China University of Geosciences
Wuhan, Hubei 430072, P. R. China
Email: [1]bk_he@126.com, [2]kang_whu@yahoo.com

ABSTRACT

Parallel verification of programs is a relatively new research area. In this paper, we first introduce our modeling approach to Hoare's logic, and then present an algorithm for parallel verification. The result indicates: Hoare's logic and model checking techniques can be thoroughly combined within finite state automatons. Besides, the obtained model has a potential for parallel verification of programs over arbitrary granularity.

Keywords: Program Verification, Parallel Verification, Hoare's Logic, Model Checking, Finite State Automaton.

1. INTRODUCTION

Program verification is classically considered difficult and resource consuming. To cope with theoretical complexity results [1-2], much attention has been devoted in recent years to parallel verification techniques and combinations of different approaches [3-5]. This paper follows the same direction. It first introduces our modeling approach to Hoare's logic [6-8], and then illustrates how to parallelize verification process. Since Hoare's logic and model checking [2, 8-10] are of different kinds of formal approaches, this work, as one might imagine, helps preserving their advantages. Although there are many other works [11-20] dealing with this topic, they differ from ours in either methodology or functionality. For instance, our work pays more attention to proof reusing and organizing methodology. Besides, it also provides a potential for parallel verification of programs over arbitrary granularity. Of course, this work relies on theorem-proving.
The paper is organized as follows: We give a presentation of related work in section 2. Sections 3 and 4 describe both our verification task and method, respectively. Section 5 demonstrates our approach, and finally section 6 states the conclusion.

2. RELATED WORK

Recently there has been increasing interest in parallelizing and distributing verification techniques [11-16]. Debashis Sahoo et al. have shown and explained in [11] why a naive parallelization of POBDD-based reachability analysis has no significant improvement on verification performance. To address this problem, the major concern of their paper is to improve the parallelism. The two crucial techniques involved in their approach for SMP architectures are early communication and partial communication. In [12], Hubert Garavel et al. deal with parallel state space construction. Their method can be described as two parts: parallel computing of local LTSs and merging of them into a global LTS. Paper [16] is devoted to improve verification performance using technique like parallel assignments to reduce state space. For example, it first compresses single assignments into parallel assignment blocks in the circumstance of weakest precondition computations, and conducts the abstraction and modeling steps subsequently. Up to now, advances in parallel verifications are mainly reported in area of model checking. And the properties of interest in these approaches are all expressed by some kind of temporal logic. For details about model checking, one can refer to [8-10].

Contrary to them, our work is based on Hoare's logic. In Hoare's system, a Hoare's formula is of the form {P} S {Q}, where both P and Q are logic formulae, called pre/post condition; and S represents a program segment. {P} S {Q} means given that P holds, if the execution of S terminates, then Q will hold. Hoare's logic includes 5 proof rules [6-8]. Based on them, we can carry out verification. However, we often use proof tableaux [8] in place of tree-like proof styles in practice.

Roughly formal verification methods include proof-based approaches like Hoare's logic, Dijkstra's approach [21] and model based checking techniques. The former kind has advantage of powerful expressiveness over the latter, but lacks automation. For example, "Hesselink", let's cite it here from [22], "regards Hoare triples as the most adequate way to specify systems." Thus combining theorem proving and model checking in a way that preserves their advantages while each compensates for the deficiencies of the other becomes a very attractive idea. John Rushby, Edmund M. Clarke and Jeannette M. Wing, to name only a few, all take sides with this [2, 17].
There are many works, e.g. [16-20], dedicated to the combination of these frameworks. Typical systems are PVS, SteP, etc. Bernhard Beckert, et al. proposed and commented on several approaches in [19]. These are global abstraction, construction, replay, similarity guided methods and his own method. Common to all of them is the use of various techniques for proof construction. For instance, his method relies strongly on what was called the similarity assessment. Apparently, this differs from our recent results covered mainly in [20] and the present paper. Although we deal with proof reusing, our focus are particularly on the proof relating and organizing methodology. As one can see in sec.5, once the model is established, we can verify programs by checking passages possibly within it, and enjoy comforts forever.

In paper [20], we deal with theoretical result. The present paper centers on its parallel application. Based on some partitioning strategy for verification task, we can easily design a parallel algorithm. To our knowledge, our work is the first to combine them within automatons [23-24]. Moreover, this approach provides a potential for parallel verification of programs over arbitrary granularity.

* This work was supported by the National Natural Science Foundation of China under Grant No. 60473081.

3. STATEMENT OF TASK

This section will define the verification task, a set TP* of Hoare's formulae, under a closed environment. For the sake of brevity, our discussion adopts functional form in place of assignment statement.

Definition 1. A generalized Hoare's formula (generalized formula for short) is of the form: $P\{f\}_G Q$, where f is a program fragment, and P, Q, called the generalized pre- and post-conditions of f, are such sets of logic expressions or predicates that for each $q \in Q$, there exists at least one element $p \in P$ satisfying $\{p\}\ f\ \{q\}$ (a Hoare's formula, also named as an instance of that generalized formula), and vice vesa.
So, for a given set H of Hoare's formulas, say $\{\{P_1\}\ f\ \{Q_1\}, \{P_2\}\ f\ \{Q_2\},\ \{R_1\}\ g\ \{W_1\}, \{R_2\}\ g\ \{W_2\}\}$, we can group them in accordance with program fragments, therefore getting the corresponding set of the generalized formulas, denoted $G_H = \{\ \{P_1, P_2\}\ \{f\}_G\ \ \{Q_1, Q_2\}\ ,\ \{R_1, R_2\}\{g\}_G\{W_1, W_2\}\ \}$. We also call G_H the generalized representation of H. It should be pointed out that the generalized representation of a given H is unique.

Definition 2. Given a set H of Hoare's formulae. A Hoare's formula $\{\wedge S\}\ f\ \{\wedge R\}$ is an instance of a generalized formula $P\{f\}_G Q$ under H, if S, R are two nonempty subsets of P and Q satisfying that: for each $r \in R$, there exists a $s \in S$ such that $\{s\}\ f\ \{r\} \in H$. Here $\wedge X$ stands for a conjunction of all elements in X.

Definition 3. Given a set H of Hoare's formulae, G_H its generalized representation. *TP** is such a set of Hoare's formulae that whose elements are those obtained by using the construction rules below, and only those, finitely many times. And an element in *TP** is also called a generalized sequent of H, or provable under G_H, a generalized closed environment.

(1) $\{\wedge S\}\varepsilon\{\wedge S\}$ in *TP** for each nonempty subset S of a generalized (either pre- or post-) condition P of some generalized formula in G_H. Where ε stands for the empty statement;
(2) Any instance of some generalized formula in G_H under H is also in *TP**;
(3) $\{\wedge P\}f;g\{\wedge W\}$ in *TP**, if $\{\wedge P\}f\{\wedge Q\}$ and $\{\wedge R\}g\{\wedge W\}$ are elements in *TP** satisfying that: for each r in R, there exists an element q in Q such that $\vdash q \to r$. Note that when in need we also omit the compositional operator ";" between "f" and "g".

4. PARALLEL VERIFICATION

This section first introduces our recent theoretical result [20], and then deals with parallel verification.

4.1. Model for Task

Definition 4. Given H, G_H as described above, and a finite state transition graph G = <V, E> whose vertices of V are generalized (pre-/post-)conditions or sets of logical expressions, and edges of E are labeled either by f , a program fragment of some generalized formula in G_H , or by ε. A possible path, say $V_1\ f_1\ V_2\ f_2\ \ldots\ f_{n-1} V_n$, in G is called a passage, if it satisfies the following two conditions for some nonempty set $P(\subseteq V_1)$. Where Vis are the vertices of the graph. In this case, we also call the string α (= f1 f2 … fn-1) concatenated from edge labels along the passage a generalized body, and m (Vi) the maximum expansion of f1 f2 … fi-1 on P. The two restrictions are:

(1) $m(V_1) = P \neq \varnothing$;
(2) For each $i (2 \le i \le n)$, if V_{i-1} ,V_i is linked by ε, $m(V_i) = \{\ x \in V_i \mid \exists p \in m(V_{i-1})(p \to x)\ \} \neq \varnothing$; and otherwise if linked by f, then $m(V_i) = \{\ x \in V_i \mid \exists p \in m(V_{i-1})\ (\{p\}\ f\ \{x\} \in H)\ \} \neq \varnothing$.

Definition 5. Given H , G_H , and a finite state transition graph G=<V, E> as described above. The graph G is called a generalized model of *TP** under H, denoted *GM(H)*, if for nonempty subsets P and Q of some two vertices (generalized conditions), $\{\wedge P\}\ f\ \{\wedge Q\} \in TP^*$ $\Leftrightarrow$ there exists a passage in *GM(H)* with f as the generalized body and Q a subset of the maximum expansion of f on P.

Definition 6. Given two sets P , Q of logic expressions or predicates, they satisfy the generalized p-implication, denoted $P \xrightarrow[p]{} Q$, if there exist two nonempty subsets $S_1 \subseteq P$ and $S_2 \subseteq Q$ such that $S_2 = \{q \in Q \mid \exists p \in S_1 (p \to q)\} \neq \varnothing$.

Theorem 1. Given H, G_H as described above, there exists a generalized model *GM(H)* for *TP**.

Proof. Without loss of generality, assuming the set of predicates involved in H is $\{P_1, P_2, \ldots, P_n, Q_1, Q_2, \ldots, Q_n\}$, and $G_H = \{\ R_i\ \{\ f_i\ \}_G\ W_i \mid\ 1 \le i \le m\ \}$. We first construct the model, and then present the proof.

Step 1: Constructing the generalized model *GM(H)*.

(1) Drawing node for each set of predicates in $\{R_i \mid 1 \le i \le m\} \cup \{W_i \mid 1 \le i \le m\}$;
(2) Drawing an arrow identified by f from R to W, if $R\{f\}_G W \in G_H$;
(3) Drawing an arrow identified by ε from X_i to Y_j, if $X_i \xrightarrow[p]{} Y_j$. Where X, Y are either R or W.

The obtained directed graph is the model $GM(H)$.

Step 2: Proving that for nonempty subsets K, L of some generalized conditions, $\{\wedge K\}\ f\ \{\wedge L\}\ \in\ TP^*$ $\Leftrightarrow$ there exists a passage in *GM(H)* with f as the generalized body, and L a subset of its maximum expansion on K.

=>: By induction on the composition.

(i) Basis: for rules 1 through 2 in def. 3, it is trivial.

(ii) Inductive step: supposing $\{\wedge K\}f_1\{\wedge P\}$, $\{Q\}f_2\{\wedge L\} \in TP^*$. By induction hypothesis, we have two passages, say $R_1 e_1 R_2 e_2 \ldots e_{u-1} R_u$, $W_1 g_1 W_2 g_2 \ldots g_{n-1} W_n$, in *GM(H)* with $f_1 = e_1 e_2 \ldots e_{u-1}$, $f_2 = g_1 g_2 \ldots g_{n-1}$ as their generalized bodies, $\varnothing \neq m(R_i) \subseteq R_i$ $(1 \le i \le u)$, $\varnothing \neq m'(W_j) \subseteq W_j$ $(1 \le j \le n)$ as the corresponding maximum expansions of $e_1\ e_2 \ldots e_i$, $g_1\ g_2 \ldots g_j$ on K and Q, i.e. $K = m(R_1)$, $Q = m'(W_1)$ respectively, and $P \subseteq m(R_u)$, $L \subseteq m'(W_n)$. Thus if the two Hoare's formulae can be combined into $\{\wedge K\}\ f_1 f_2\ \{\wedge L\} \in TP^*$, i.e. for each q in Q , there exists a p in P such that $\vdash p \to q$, we have $\varnothing \neq Q = m'(W_1) \subseteq \{w \in W_1 \mid \exists p \in P(p \to w)\} \subseteq \{w \in W_1 \mid \exists p \in m(R_u)(p \to w)\} = m(W_1)$. By definition 6 and the picturing rule for *GM(H)*, it follows easily $R_u \xrightarrow[p]{} W_1$, and therefore existing a ε arrow leading from R_u to W_1. Consequently, we can construct a new maximum expansion $m(W_j)$ of $(g_1 g_2 \ldots g_{j-1})$ on $m(W_1)$ which satisfies:

$\varnothing \neq m'(W_j) \subseteq m(W_j)$ for $1 \le j \le n$. So combining them with those (m_i's) of f_1, and again by induction hypothesis, we get the proof of the path $R_1\ e_1\ R_2\ e_2\ \dots\ e_{m-1}\ R_m\ \varepsilon\ W_1 g_1 W_2 g_2 \dots g_{n-1} W_n$ being a passage with $m(R_1) = K$ and $L \subseteq m(W_n)$. This is the desired result.

<=: By induction on the number of the edges along the concerned passage.

(i) Basis: when a passage contains only one edge, the proof is trivial.

(ii) Inductive step: let $V_1\ e_1 V_2\ e_2\ \dots\ e_{n-1} V_n\ x V_{n+1}$ be a passage in *GM*(*H*) with $f = e_1\ e_2\ \dots\ e_{n-1} x$ as the generalized body, and $m(V_1) = K \neq \varnothing, \varnothing \neq L \subseteq m(V_{n+1})$. Where V_is stand for generalized conditions, and e_is along with x for edge labels. By induction hypothesis, we have $\{\wedge K\}\ e_1 e_2\ \dots\ e_{n-1} \{\wedge m(V_n)\}$, $\{\wedge m(V_n)\} x\ \{\wedge L\} \in TP^*$. Again from definition for TP^*, it follows $\{\wedge K\}\ f\ \{\wedge L\} \in TP^*$, the desired result. □

4.2. Parallel Algorithm

Theorem 1 provides a model suitable not only for verifying but also for generating reliable programs. Now let's discuss how to verify programs with components from a given set *H* in parallel style.

Algorithm 1 Given $H = \{\{X_j\} f_j \{Y_j\} \mid 1 \le j \le k\}$, G_H, *GM(H)* as above. Let the *goal* to be verified be $\{P\}\alpha\{Q\}$, where $\alpha = f_1 f_2 \cdots f_n \in \{f_1, f_2, \cdots, f_k\}^*$. The parallel verification algorithm is as follows.

(1) Solve $m(Z_1) = \{x \in Z_1 \mid (P \rightarrow x)\}$ for $Z_1\ \{f_1\}_G\ W_1 \in G_H$. Because there exists only one edge in *GM(H)* with label "f_1".

(2) Calculate the maximum expansion of α using the algorithm of Fig.1.

```
CalculateExpansion(goal, H, GM(H))
Begin
  Let |goal| be the length of α ;
  Divide α into 2 halves: lHalf and rHalf;
  Let Z_i {f_i}_G W_i ∈ G_H (1 ≤ i ≤ k );
  Solving R = {(t,e_t)|t ∈ Z_|goal|/2 +1, e_t is the maximum
     expansion of rHalf on {t} ⊆ Z_|goal|/2 +1 }.
//if the path corresponding to rHalf doesn't form
//a passage, return {"No"}
  Solving R'= (P, E_P). Where E_P is the maximum expansion
     of lHalf on P;
//if the path corresponding to lHalf doesn't form
//a passage, return {"No"}
  if there is no ε arrow linking W_|goal|/2 and Z_|goal|/2 +1
    then return( {"No"})
    else
      begin
        If E_P , R ≠ ∅ then
          Begin
            Solving E_P'= {x ∈ Z_|goal|/2 +1| ∃ p ∈ E_P (p → x)} ;
            Solving Q'= ⋃_{t∈E_p'∧(t,e_t)∈R} e_t
          End;
          else Q':= ∅ ;
        Return(Q')
      end
  end;
```

Fig.1. Parallel computation of the maximum expansion

(3) Check the returned result. If {No}, then the goal to be verified is incorrect with respect to G_H; if $\vdash \wedge Q' \rightarrow Q$, then $\{P\}\alpha\{Q\}$ is partially correct; otherwise, the goal is unprovable under G_H. □

Note that the solving processes for both R and R' can be parallelized. In fact, the parallelism rooted in the model provides convenience to define the relational property of each component (or even compositional component), therefore supporting parallel computations over arbitrary granularity. To be understanding, we can visualize step 2 as follows.

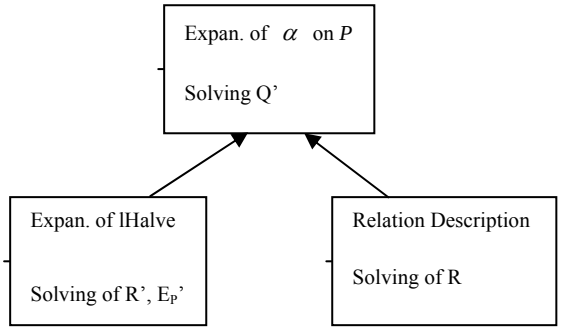


Fig.2. Composition of expansions

4.3. Parallel Verification of General Programs

The principle for applying linear model to cases like both branching and iterative structures is: verifying program fragments level by level, i.e. first some inner level and then its outside. The sketch of the method forms the following algorithm.

Algorithm 2. Given a *GM(H)*, to verify an arbitrary program *p* with components from *H*, we can proceed incrementally, and level by level as follows.

(1) Collecting all iterations and if-statements in *p*, denoted *I B*(*p*).

(2) Invoking algorithm 1 to verify elements in *I B*(*p*) of *k* levels based on the present *GM(H)*.

(3) Maintaining *GM(H)* by adding the verified results of step 2 as either new generalized formulas or properties into the present *GM(H)*;

(4) *k* := *k*+1. If there is some element of *k* levels in *IB*(*p*) remaining untouched, back to 2);

(5) Verifying *p* based on the ultimate *GM(H)*. □

Clearly, verification proceeds in parallel in each level. Of course, we should regard "if" and "while" statements as the same grammar unit when defining the concept "level". By the way, apart from theorem proving, all algorithms are effective. For example, to count the complexity of step 2 in algorithm 1, we need just take notice of the three "solving" sub-steps and definitions 3 through 4. Def. 6 is also compatible with them.

5. EXAMPLE

This section will demonstrate our approach by verifying two programs constructing from a given set of components (Hoare's formulae). Since this method is a component based approach, we also assume the implementations of components are transparent.

Example 1. Given two programs and *H* of Hoare's formulae as shown in Fig.3 and Table 1. Asking whether they are partially correct. Where all the involved variables are nonnegative integers.

Program 1: $\{P_1 \wedge P_5\}$ while $u \neq 0$ do begin f1; f4; f2 end $\{P_1 \wedge P_5 \wedge u=0\}$
Program 2: $\{P_7\}$ while $r \geq z$ do begin f1;f3; f2; f4 end $\{P_7 \wedge r < z\}$

Fig.3. The two programs to be verified

Table 1. The set *H* of Hoare's formulae. Here each row stands for a Hoare's formula.

Pre-condition		Function	Post-condition	
P_1	$y+uz=xz$	f1	$y+(u-1)z=xz$	P_4
P_2	$u>0$	f1	$u>0$	P_2
P_3	$x=r+qz \wedge r \geq z \wedge z>0$	f1	$x=r+qz \wedge r \geq z \wedge z>0$	P_3
P_4	$y+(u-1)z=xz$	f2	$y+uz=xz$	P_1
P_2	$u>0$	f2	$u \geq 0$	P_5
P_6	$x=r+(q+1)z \wedge r \geq 0 \wedge z>0$	f2	$x=r+(q+1)z \wedge r \geq 0 \wedge z>0$	P_6
P_3	$x=r+qz \wedge r \geq z \wedge z>0$	f3	$x=r+(q+1)z \wedge r \geq 0 \wedge z>0$	P_6
P_4	$y+(u-1)z=xz$	f3	$y+(u-1)z=xz$	P_4
P_2	$u>0$	f3	$u>0$	P_2
P_6	$x=r+(q+1)z \wedge r \geq 0 \wedge z>0$	f4	$x=r+qz \wedge r \geq 0 \wedge z>0$	P_7
P_1	$y+uz=xz$	f4	$y+uz=xz$	P_1
P_5	$u \geq 0$	f4	$u \geq 0$	P_5

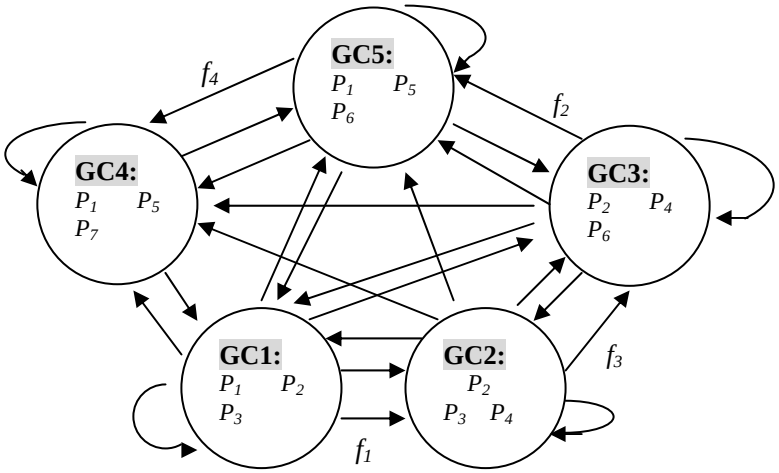


Fig.4. The generalized model *GM(H)* for *TP** under *H*.
Where GC_is stand for the generalized conditions, and arrows without labels for ε edges.

Verification. Constructing both the generalized model *GM(H)* (fig.4) as done in theorem 1 and goals to be verified. By step 1 of algorithm 1, we can transform original problems into such ones as whether $\{\wedge m(GC_1)\}$ f1; f4; f2 $\{\wedge X\}$ and $\{\wedge m'(GC_1)\}$ f1;f3; f2; f4 $\{\wedge Y\}$ for some subsets X, Y of GC_4 are in *TP** satisfying $\vdash \wedge X \rightarrow (P_1 \wedge P_5)$, $\vdash \wedge Y \rightarrow P_7$ respectively. If there is no problem for some of the two goals, it follows from iteration rule of Hoare's logic that goal is partially correct. Because $(P_1 \wedge P_5) \rightarrow \wedge m(GC_1)$ and $P_7 \rightarrow \wedge m'(GC_1)$ hold. Now let's demonstrate our approach based on the *GM(H)*.

Step 1: Solving $m(GC_1)$ and $m'(GC_1)$, we have $m(GC_1)= \{x \in GC_1 \mid (P_1 \wedge P_5 \wedge u \neq 0) \rightarrow x\} = \{P_1, P_2\}$, and $m'(GC_1) = \{x \in GC_1 \mid (P_7 \wedge r \geq z) \rightarrow x\} = \{P_3\}$.

Step 2: Invoking *CalculateExpansion*($\{\wedge m(GC_1)\}$ f1; f4;f2 $\{P_1 \wedge P_5\}$, *H, GM(H)*) and *CalculateExpansion*($\{\wedge m'(GC_1)\}$ f1;f3; f2; f4$\{P_7\}$, *H*, *GM(H)*), we get {"No"} and $Y = \{P_7\}$ respectively.

Step 3: Obviously, the first goal is incorrect. Since applying algorithm 1 to it returns {"No"}. However the second program is correct. Because $\{\wedge m'(GC_1)\}$ f1;f3;f2;f4 $\{\wedge Y\} \in TP^*$, i.e. it is correct. Again $\vdash \wedge Y \rightarrow P_7$ holds. This means $m'(GC_1)\}$ f1;f3; f2; f4 $\{P_7\}$ holds. Again by step 2 : $(P_7 \wedge r \geq z) \rightarrow \wedge m'(GC_1)$, we have $\{P_7 \wedge r \geq z\}$ f1;f3;f2;f4 $\{P_7\}$. By Hoare's logic, it follows the result. □

Besides, we can also see from theorem 1 that *while z <= r do begin* $(f_1;)^* f_3$; $(f_2;)^* f_4$ *end* is equivalent to program 2 (fig.3) with respect to their corresponding pre- and post-conditions given in fig.3. Because the passage $(GC_1\ f_1\ GC_2\ \varepsilon)^* GC_2\ f_3\ GC_3\ \varepsilon\ (GC_3\ f_2\ GC_5\ \varepsilon)^*\ GC_5\ f_4\ GC_4$ satisfies and verifies : $(P_7 \wedge r \geq z) \rightarrow P_3$, $\{P_3: x=r+qz \wedge r \geq z \wedge z>0\}$ $(f_1;)^* f_3; (f_2;)^* f_4$ $\{P_7\} \in TP^*$. So, we have $\{P_7 \wedge (r \geq z)\}$ $(f_1;)^* f_3; (f_2;)^* f_4$ $\{P_7\}$, i.e. $\{P_7\}$ *while* $r \geq z$ *do begin* $(f_1;)^* f_3; (f_2;)^* f_4$ *end* $\{P_7 \wedge z > r\}$, the desired result.

6. FUTURE WORKS

This paper introduces our recent advances in both modeling problems about Hoare's logic and parallel verification. If well equipped with modern ATP (Automated Theorem Proving) techniques [25-27], the novel approach may possibly become an alternative way to face software reliability. Our future work includes: merging boolean expressions with existing models, investigating both new verification tasks and modeling methods, implementing an experimental environment, etc. We believe the structure of G_H together with its operators has a great influence on the automation.

REFERENCES

[1] Tony Hoare. The Verifying Compiler: A Grand Challenge for Computing Research, LNCS 2622, 2003, pp.262~272

[2] Edmund M. Clarke, Jeannette M. Wing. et.al. Formal Methods: State of the Art and Future Directions. ACM Computing Surveys. 28, 1996. pp.626~643

[3] Lubos Brim, Orna Grumberg. Introductory Paper. Int. J. Softw Tools Technol Transfer. 7:1-3, 2005. pp.1~3

[4] Ahmed Bouajjani. Languages, Rewriting Systems, and Verification of Infinite-State Systems. F. Orejas, P. G. Spirakis, and J. van Leeuwen (Eds.): ICALP 2001, LNCS 2076, 2001. pp.24~39

[5] Jacek Blazewicz, Maciej Drozdowski, Mariusz Markiewicz. Divisible Task Scheduling: Concept and Verification. Parallel Computing. 25, 1999. pp.87~98

[6] C. A. R. Hoare, An Axiomatic Basis for Computer Programming, CACM, 12, 1969. pp.576~583

[7] Zohar, Manna. Mathematical Theory of Computation. McGraw-Hill, 1974.

[8] Michael Huth , Mark Ryan. Logic in Computer Science: Modelling and Reasoning about System. Cambridge University Press, England, 2004.

[9] Gerard J. Holzman, Margaret H. Smith. Software Model Checking: Extracting Verification Models from Source Code. System Testing, Verification and Reliability. 11, 2001. pp.65~79

[10] Willem Visser, Klaus Havelund, Guillaume Brat, SeungJoon Park, Flavio Lerda. Model Checking Programs. Kluwer Academic Publishers: Netherlands, 2002.

[11] Debashis Sahoo, Jawahar Jain, Subramanian Iyer, and David Dill. A New Reachability Algorithm for Symmertic Multi-Processor Architecture. D. A. Peled and Y. K. Tsay (Eds.): ATVA 2005, LNCS 3707, 2005. pp.26~38

[12] Hubert Garavel, Radu Mateescu, and Irina Smarandache. Parallel state Space Construction for Model Checking. M. B. Dwyer (Ed.): SPIN 2001, LNCS 2057, 2001. pp.217~234

[13] Michael D. Jones, Jacob Sorber. Parallel Search for LTL Violations. Int. J. Softw Tools Technol Transfer. 7, 2005. pp.31~42

[14] Tamir Heyman, Danny Geist, Orna Grumberg, and Assaf Schuster. A Scalable Parallel Algorithm for Reachability Analysis of Very Large Circuits. Formal Methods in System Design, 21, 2002. pp.317~338

[15] W.-C. Liu and C.-G. Chung. Path-Based Protocol Verification Approach. Information and Software Technology. 42,2000. pp.229~224

[16] Murray Stokely, Sagar Chaki, Joel Ouaknine. Parallel Assignments in Software Model Checking. Electronic Notes in Theoretical Computer Science. 157, 2006. pp. 77~94

[17] John Rushby. Theorem Proving for Verification. F. Cassez et al. (Eds.) : MOVEP 2000, LNCS 2067, 2001. pp.39~57

[18] Weiqiang Kong, Kazuhiro Ogata, Takahiro Seino, and Kokichi Futatsugi. A lightweight Integration of Theorem Proving and Model Checking for System Verification. Proc. of the 12th Asia-Pacific Software-Engineering Conference (APSEC'05), 2005.

[19] Bernhard Beckert, Vladimir Klebanov. Proof Reuse for Deductive Program Verification. Proc. of the Second International Conference on Software Engineering and Formal Methods (SEFM'04), 2004.

[20] He Pei, Kang Lishan and Li Qiongzhang. Model for Parallel Verification of Programs. SNPD'07, IEEE Computer Press, 2007. (To appear)

[21] E. W. Dijkstra. A Discipline of Programming. Prentice-Hall, 1976.

[22] Awadhesh Kumar Singh, Umesh Ghanekar, Anup Kumar Bandyopadhyay. Specifying Mobile Network Using a wp-like Formal Approach. Revista Colombiana de Computacion, 6:2, 2005. pp59~77.

[23] Alfred V. Aho, Ravi Sethi, Jeffrey D. Ullman. Compilers: Principles, Techniques, and Tools. Pearson Education, Inc, 1986.

[24] John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman. Introduction to Automata Theory, Languages, and Computation. Pearson Education, 2001.

[25] Geoff Sutchiffe's Overview of Automated Theorem Proving. (http://www.cs.miami/~tptp)

[26] Theorema. (http://www.theorema.org)

[27] Automated Deduction Systems and Groups. http://www-unix.mcs.anl.gov/AR/others.html

Pei He is a Ph. D student of the State Key Laboratory of Software Engineering, Wuhan University. He graduated from Wuhan University and The Institute of Software, Academia Sinica in 1986 and 1989 respectively, with specialty of computer science. His research interests are in formal methods, compiler, and programming language. He has published over 10 Journal papers.

Lishan Kang is a Full Professor, Dean, and Honorary professor at Computer School, Wuhan University, Computer School, China University of Geosciences, and Nanjing University of Aeronautics and Astronautics respectively. His research interests center on theoretical computer science and mathematics. He has hosted many NSF projects (including 2 key projects), authored 7 influential books, and published more than 300 research articles. His academic activities and positions include Director of The State Key Lab of Software Engineering, Vice Chair of the Subdivision on Theoretical Computer Science, Computer Society of China, Academic Leaders of some national key institutes, Members of several international journal editorial boards, and Chairs of several important international conferences, to name but a few. Due to his academic contribution, he wins many prizes from Chinese government.

A Parallel Algorithm for Solving Tridiagonal Linear Systems*

Xiping Gong, Junqiang Song, Lilun Zhang, Wentao Zhao, Jianping Wu
School of Computer Science, National University of Defense Technology ChangSha, China, 410073,
Email: gongxpjia@163.com

ABSTRACT

Parallel solving tridiagonal linear systems is the bottleneck to parallel deal with most of scientific and engineering problems. In this paper, we develop a new parallel algorithm of tridiagonal linear systems. The parallel algorithm only needs $O(13n)$ float operations and one global communication round with a pretreatment. The amount of data transmitted in communication round is equal to the number of processors and independent of n. In addition to showing its theoretical complexity, we have implemented this algorithm on a real distributed memory parallel machine. In theory it can be use to solve arbitrary tridiagonal linear systems correctly and efficiently.

Keywords: Parallel Algorithm, Tridiagonal Linear Systems

1. INTRODUCTION

The original motivation for this paper are some intriguing questions arising in the parallel solution of tridiagonal linear equations. Nowadays, many direct factorization methods fitting for parallelization have been developed, including the Stone's "scan-based" algorithm[1], "odd-even cyclic reduction"[2] and "partitioning"[3] [4]. At the first glance, these methods seem to be efficient. But for distributed memory parallel computing, they may cause great communication overhead with high communication requirements. In parallel computing, the time used by these methods is even more greater than that of some optimal sequential methods such as LU factorization method because of the communication time is usually much greater than computation time. We point that the reason of this is that the special structure of the matrix has not been fully used. In fact, the effort to reduce communication is centered on reducing the number of communication rounds. In this paper, we take account of the special characteristic of the tridiagonal matrix, and present an efficient parallel algorithm for solving tridiagonal systems. The new algorithm needs $O(13n)$ (n is the scale of the problem) float operations and one global communication round, by using a pretreatment to get N_p directions which is the number of the processors used to parallel compute. We also demonstrate how to implement the method on a parallel computer to obtain high efficiency. It should be emphasized that in this paper we adopt a purely algebraic viewpoint for the reason that our intention is to illuminate the algebraic structure that enables parallelism. Other numerical behavior of the new method, such as stability, will be discussed in future work.

The paper is organized as follows: In section 2 we will present the parallel algorithm. Algorithm analysis and computational complexity will be discussed in Section 3. Numerical experiments are given in section 4. In Section 5, we finally get a conclusion and some remarks for the new parallel algorithm.

* This work was supported by National Nature Science Foundation under grant number 40505023.

2. DERIVATION OF THE METHOD

2.1 Problem

A tridiagonal linear system of equations is described by the tridiagonal matrix A with coefficients shown below,

$$A=\begin{bmatrix} a_1 & b_1 & & & \\ c_2 & a_2 & b_2 & & \\ & c_3 & a_3 & \ddots & \\ & & \ddots & \ddots & b_{n-1} \\ & & & c_n & a_n \end{bmatrix}.$$

The system of equations associated a tridiagonal matrix A is

$$Ax = r \qquad (1)$$

$x, r \in \Re^n$ are column vectors and matrix A is nonsingular. In order to describe the parallel algorithm we denote N_p as the number of the processors for parallel computing and N_p is an even number.

2.2 Data Partition

Assuming that the tridiagonal linear system is distributed on a number of processors, so that each processor owns a contiguous part of rows. There are two kinds of data parts just like fig 1 and fig 2.

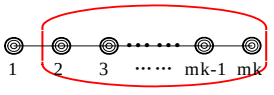


Fig.1. Data Part

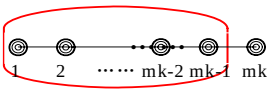


Fig.2. Data Part

All data can be arranged in a sequence of data partition like fig 3 that the first part is like figure 1 and the last part is like fig 2 which is an alternating sequence of the two kind parts.

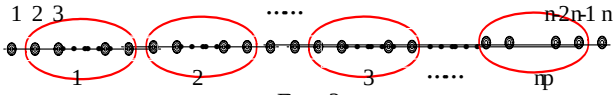


Fig.3. A Sequence of Data Partition

The parallelism of the partition is N_p which is the number of the processors. In parallel computing, every part will be assigned to one processor. Each processor will compute one point which is not in the red circle and all points in the red circle which were allocated to it. The points can be arranged two sets, one is in the red circles and the other is not. We denote the points in the red circles as set I and the points not in the red circles as set J. Obviously, if we have known the value of the points which are not in the red circles the value of the points in the red circle can be computed directly and easily just using forward or backward substitution. This is the basic idea of the parallel algorithm and how to compute the value of the points not in the red circle is the key of the parallel algorithm. Next in section 2.3 we will introduce how to compute them.

2.3 Compute the Value of the Points Not in the Red Circles

Let matrix A is nonsingular, if $p_1, p_2, \cdots, p_n \in \Re^n$ are linearly independent vectors, then $Ap_1, Ap_2, \cdots, Ap_n \in \Re^n$ must are linearly independent vectors. The solution x of the system (1) can be linearly expressed as follows:

$$x = \sum_{i=1}^{n} \alpha_i p_i \cdot \quad (2)$$

The vector $p_i, i = 1,2,\cdots,n$ is called the direction. of the solution can be decomposed.

Therefore we can get

$$Ax = A(\sum_{i=1}^{n} \alpha_i p_i) = \sum_{i=1}^{n} \alpha_i Ap_i = b$$

from (1) and (2) just by some simple linear algebra knowledge. That's to say if we can find the right term b 's linear expression about the linearly independent vectors $Ap_1, Ap_2, \cdots, Ap_n \in \Re^n$

$$b = \sum_{i=1}^{n} \alpha_i Ap_i, \quad (3)$$

we can obtain the solution of the linear system (1) directly by using the formula (2).

Choosing a set basis of the space $\Re^n$ just like $e_i \in \Re^n, i \in I$ and $p_j \in \Re^n, j \in J$, satisfying

$$e_i(j) = \begin{cases} 0, & j \neq i \\ 1, & j = i \end{cases}$$

and

$$(Ae_i, Ap_j) = 0, i \in I, j \in J, \quad (4)$$

the formula (2) can be transformed to

$$x = \sum_{i \in I} \alpha_i e_i + \sum_{i \in J} \alpha_i p_i \cdot \quad (5)$$

We can see the value on the points which are not in the red circles only have relations with the vectors $p_j, j \in J$. So the problem to compute the values on the points not in the red circles is equivalent to computing the values of $\alpha_i, i \in J$.

In fact from (4), (5) and the property that there are only one group $\alpha_i, i \in I, i \in J$ satisfying (3), we obtain

$$\begin{cases} (\sum_{j \in I} \alpha_j Ae_j, Ae_i) = -(b, Ae_i), i \in I & (6) \\ (\sum_{i \in J} \alpha_i Ap_i, Ap_j) = -(b, Ap_j), j \in J. & (7) \end{cases}$$

It's obvious that (6)–(7) can be cut into two different independent linear systems, one is (6) just having the variables $\alpha_i, i \in I$ and the other one is (7) just having the variables $\alpha_i, i \in J$. In order to compute the value of the point which is not in the red circles we only need to solve the second linear system (7). There are only N_p points which are not in the red circles that is as many as the number of the processors for parallel computing, it's clear from figure 3. That's to say the linear system (7) only has N_p variables.

If N_p is large we can use some suitable parallel methods to solve (7). Usually $N_p << n$, so we don't care about how to solve the linear system (7).

After solving the linear system (7), we can get the points' value which are not in the red circles using the following formulary

$$x^i = \sum_{j \in J} \alpha_j p_j^i, i \in J, \quad (8)$$

where x^i denotes the i th point's value and p_j^i denotes the i th position's value of vector p_j. By this time we could depict the parallel algorithm completely.

2.4 Description of the Parallel Algorithm

Suppose we have got the directions p_j and $Ap_j, j \in J$, the parallel algorithm consists of the following five steps:

(1) Each processor computes the right term $-(b, Ap_j)$ of the linear system (7) about the point what was allocated to it and is not in the red circle.
(2) Communicate to each other in order to get all the right term of the linear system (7) on every processor.
(3) Each processor uses suitable method to solve linear system (7).
(4) Each processor uses (8) to compute the needed data x^i.
(5) Each processor computes the points' values in the red circle of it's own just using forward or backward substitution.

By now we have obtained the new parallel algorithm, but we must choose a group basis of the space $\Re^n$ just like $e_i \in \Re^n, i \in I$ and $p_j \in \Re^n, j \in J$ and these basis satisfy (4). We call the process to get the group basis and to get the coefficient matrix of linear system (7) as pretreatment.

2.5 Pretreatment

The only thing we should do is to construct the group basis and get the coefficient matrix of linear system (7). Firstly, we choose a group basis of $\Re^n$ which are $e_i, i = 1,2,\cdots n$. Since A is a tridiagonal matrix, it has an important special characteristic that

$$(Ae_i, Ae_j) = 0, |i - j| > 2, i, j = 1,2,\cdots,n. \quad (9)$$

In order to get a group basis which satisfy (4), we choose $e_i, i \in I$ as before and $p_j, j \in J$ as the following formulary

$$p_j = e_j + \sum_{i \in I} \beta_i e_i, j \in J \cdot \quad (10)$$

Ax is a linear transformation, it's obvious that

$$Ap_j = Ae_j + \sum_{i \in I} \beta_i Ae_i, j \in J \cdot \quad (11)$$

For every $j \in J$ we can get

$$(\sum_{i \in I} \beta_i Ae_i, Ae_k) = -(Ae_j, Ae_k), k \in I \quad (12)$$

according with (4).

From (9), it's easy to conclude that for every $j \in J$ the linear system (12) is made up by two independent parts which contain the values at the points in the two left or right neighbor red circles, and they are five-diagonal equations. For every $j \in J$ that $p_j^k = 0, k \neq j, k, j \in J$ and $p_j^j = 1.0$. When the group of basis are structured by this method, the solution of linear system (7) α_j is the solution of linear system (1) for every x^j $j \in J$. Therefore the 4th step of the parallel algorithm needn't do at all. After getting the directions $p_j, j \in J$ and $Ap_j, j \in J$, the coefficient matrix of linear system (7) can be computed directly.

3. ANALYSIS OF THE PARALLEL ALGORITHM

3.1 Analysis of the Pretreatment

The pretreatment can be dived into two parts. One is to obtain $p_j, j \in J$ and $Ap_j, j \in J$, the other one is to compute the coefficient matrix of linear system (7). In order to analysis the parallel algorithm conveniently, we suppose that N_p is an even number and n/N_p is an integer.

Every processor has contiguous number of n/N_p rows that $n/N_p - 1$ points are in the red circle and one is not. For every $j \in J$, the linear system (12) is consisted of one or two five-diagonal linear system with $2(n/N_p - 1)$ unknown elements. The first and last processor have one, others have two. That's to say we should solve $2(N_p - 1)$ five diagonal linear systems. Using LU factorization method every five diagonal linear system only needs $O(38(n/N_p - 1))$ float operations. Therefore to obtain $p_j, j \in J$ needs $O(76(N_p - 1)(n/N_p - 1))$ float operations. Computing the coefficient matrix and right term of (12) need $O(9n)$ float operations. That's all getting and solving the linear system (12) only needs $O(85n)$ float operations. From the process we known every $p_j, j \in J$ at most has $4n/N_p - 2$ nonzero contiguous elements and every $Ap_j, j \in J$ at most has $4n/N_p$ nonzero contiguous elements. To compute $Ap_j, j \in J$ at most needs $5(4n/N_p)N_p$ float operations. Computing the coefficient matrix (7) at most needs about $O(20n)$ float operations. The pretreatment just needs about $O(125n)$ float operations.

The analysis for the pretreatment is just to estimate that the pretreatment can be done at an acceptable cost. What's more, the pretreatment can be paralleled directly, because the computations for each $p_j, j \in J$ and $Ap_j, j \in J$ are independent completely. Therefore the pretreatment can be done at an acceptable cost.

3.2 Analysis of the Parallel Algorithm

From the analysis 3.1, every $p_j, j \in J$ at most has $4n/N_p - 2$ nonzero contiguous elements and every $Ap_j, j \in J$ at most has $4n/N_p$ nonzero contiguous elements. For the first and the last processor, p only has $2n/N_p - 1$ nonzero contiguous elements and Ap only has $2n/N_p$ nonzero contiguous elements. So the first step every processor at most needs $2(4n/N_p) - 1$ float operations, but for the first and the last processor need $2(2n/N_p) - 1$. The second step just needs an ALLGATHER operation. At the third step the number of float operations of solving the linear system (7) using Gaussian elimination method is $O(2N_p^3/3)$. In fact we can get the inverse of the coefficient matrix of linear system (7) firstly and then get the solution directly that only needs $(2N_p - 1)N_p$ float operations. we needn't do the 4th step at all using our method to construct the directions $p_j, j \in J$ actually. The last step needs $5(n/N_p - 1)$ float operations for each processor. Excepting the third step, the whole parallel algorithm needs $13n - 8n/N_p - 7N_p$ float operations. This result is more less than $21n$ [3] and $17n$ [4]. The big advantage is only need one global communication round. Therefore the communication time will be more less than other methods.

4. NUMERICAL EXPERIMENT

In order to show the correctness of the parallel algorithm, we take a tridiagonal linear system (1) that the coefficients are $a_i = 2, b_i = 1, c_i = 1, i = 1,2,\cdots,n$, the true solutions are $x_i^* = 1, i = 1,2\cdots,n$ and all real numbers are double precision. Two quantities are used in error analysis, one is the classical Euclidean scalar product of the difference between the solutions and the true solutions

$$d = (x - x^*)^T (x - x^*), \qquad (13)$$

the other one is the largest difference of the elements between the solutions and the true solutions

$$f = \max_{i=1,2,\cdots,n} abs(x_i - x_i^*) \qquad (14)'$$

Table 1 The correctness of the parallel algorithm

processors	n	d	f
2	12	1.458160079494464E-029	1.776356839400250E-015
4	24	1.289294541970591E-029	1.332267629550188E-015
6	30	3.546176288001330E-029	1.554312234475219E-015
8	48	3.454964245835150E-028	4.440892098500626E-015

The correctness of the parallel algorithm is shown in table 1.If we don't taken into account the communication overhead, the running time of the parallel algorithm should be proportionable to the scale of the solving problem. Table 2 give running times for the parallel algorithm on 4 processors in different scale problems. In fact, the parallel algorithm has been run 10000 times for different scale problems. The different cases used the same number of processors and communicated the same size datum, so the communication time should be kindred. The difference of the running time for the two neighbors in table 2 is almost same, that's to say the running time of the parallel algorithm is proportioned to the problem scale. We can see that the proportion of the communication time is too high from table 2 and table 3. Because of the overall computation speed is considerably larger than the overall communication speed, if the problem size is not enough large the proportion of the computation time is not high although only needs one global communication round.

Table 2 Running times for the parallel algorithm

n	20000	40000	60000	80000
time(s)	6.2862	10.0513	15.8209	19.8307

Table 3 The proportion of the computation time

n2-n1	40000-20000	60000-40000	80000-60000
time(s)	3.7651	5.7696	4.0098

There are some factors what affect the performance of this parallel algorithm. Using more processors we need to compute more vectors $p_j, j \in J$ and $Ap_j, j \in J$ and the scale of linear system (7) is increasing. As the increasing of the problem scale, the scale of linear system (12) is increasing too. It is more difficult to solve (12) and (7) with high numerical

precision. +-That's to say it's hard to guarantee that the condition (4) is satisfied with high numerical precision. Some experiments have shown that there are some problems as the increasing of the problem scale and the increasing of the processor number that may because of in the 5^{th} step it is difficult to control the error accumulation. Till now, we have implemented the parallel algorithm correctly, and we will continue to investigate the performance of this parallel algorithm in a future paper.

5. CONCLUSIONS

In this paper, we presented a parallel algorithm for solving tridiagonal linear systems with a pretreatment. The algorithm can be used for the direct solution of an arbitrary tridiagonal linear system in theory. We have analyzed in detail the implementation of our parallel algorithm. It's more useful for solving the tridiagonal linear system with the same tridiagonal coefficient matrix repeatability. From the analysis, the parallel algorithm at most needs $13n$ float operations and one global communication round that gain an advantage over most parallel algorithms for solving tridiagonal linear systems. At the same time we must do some pretreatments to get the directions $p_j, j \in J$, the vectors $Ap_j, j \in J$ and the coefficient matrix of (7). The process is time consuming than solving (1) directly though it is proportioned to the problem scale. But it is worthwhile to do when we need to solve tridiagonal linear systems repeatly which have the same coefficient matrix which is usually the case in practice.

In the future, we will continue to improve the performance of this algorithm. Our aim is to adopt our algorithm, to implementation on large scale parallel computers, by increasing the adaptability, dependability, and scalability of the solution methods.

REFERENCES

[1] H.S. Stone. "An Efficient Parallel Algorithm for the Solution of a Tridiagonal Linear System of Equations." JACM, 20:27-38, Jan. 1973.

[2] R.W. Hockney. "A Fast Direct Solution of Poisson's Equation Using Fourier Analysis." JACM, 12:95-113, 1965.

[3] H.H. Wang. A Parallel Method for Tridiagonal Equations. ACM Trans. Math. Software, 7:170-183, 1981.

[4] Michelse P H, Van der Vorst H A. Data trsport in Wang's partition method. Parallel Computing, 7:87-95, 1988.

Reliability- Based Optimum Study on FRP Laminated Plates with Genetic Algorithm*

Xiangyang Wang
School of Transportation, Wuhan University of Technology
Wuhan 430063, China
Email: wangxy2003@163.com

ABSTRACT

This paper proposes a procedure for the optimum design of composite laminates with initial imperfection under probabilistic considerations. Based on the last-ply failure criterion, a probability progressive failure mode of composite laminates is proposed to evaluate the structural reliability. Ply-level failure probability is evaluated by the first order reliability method (FORM) and system reliability is computed based on the last-ply failure criterion. A structural optimization problem is solved with the fiber orientation and the lamina thickness as the design variables, the system reliability as the objective, and genetic algorithm is used to search for the optimum solutions. The solutions on the last-ply failure are compared with those on the first-ply failure, and indicate that the former take full advantage of the material behavior than the latter.

Keywords: Laminated Composites, Reliability, Optimum, Last-ply Pailure, Genetic Algorith

1. INTRODUCTION

Laminated composite materials have become important engineering materials for the construction of automobile, machine, space and marine structures, and the optimum design of composite structures have been studied widely [1-2]. But most of them yield the optimum laminate configuration under a deterministic condition where the design variables and loads are assumed to have no variations. A number of experiments and studies have shown that composite materials exhibit wide scatter as a result of the inherent uncertainties in the design variables. Traditional deterministic methods generally use experience-bases safety factors to account for uncertain structural behavior. To take full advantage of the uncertainly of composite material behavior, a probabilistic optimum design method is required to incorporate the uncertainty in the structural analysis and design.

A number of researchers have studied the reliability of laminated composite plates with first-ply failure criterion. That is, the structure will be failure if each of the ply has been failed. But in fact, the structure may have the carrying capacity. Based on the last-ply failure criterion, Mahadevan et al. [3] and Chen et al. [4] recently have proposed a probabilistic progressive failure mode of composite laminates to estimate the ultimate strength failure probability. The overall failure of the laminate is caused by a series of ply-level failure events. There exist many possible failure sequences of the ply-level events that lead to overall laminate failure and the system failure probability is estimated by the dominant ply-level failure sequence.

On the basis of the last-ply failure criterion, this paper develops a method to estimate the composites structure's reliability. A structural optimization problem is solved with the fiber orientation and the lamina thickness as the design variables and the maximum system reliability as the objective. A numerical example is worked out to demonstrate the necessity and validity of the method.

2. STRUCTURAL ANALYSIS

Consider a simply supported symmetric laminated composite plate with initial imperfection w_0 and with an in-plane bi-axis compression loading $\{N\}$, as shown in Fig.1. The governing equation of the plate can be expressed as [4,5]:

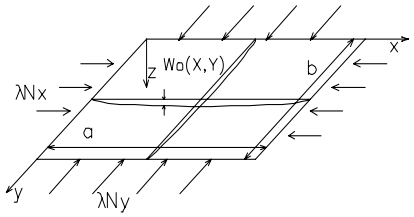


Fig.1. A laminated composite plate with an initial imperfection

$$D_{11}\frac{\partial^4 w_1}{\partial x^4}+2(D_{12}+2D_{66})\frac{\partial^4 w_1}{\partial x^2\partial y^2}+D_{22}\frac{\partial^4 w_1}{\partial y^4}=$$

$$\lambda\left\{N_x\frac{\partial^2}{\partial x^2}(w_0+w_1)+N_y\frac{\partial^2}{\partial y^2}(w_0+w_1)\right\} \quad (1)$$

where N_x and N_y are in-plane forces, λN_x and λN_y the critical values of these forces, w_0 is the initial imperfection, w_1 the deflection due to the forces, and D_{ij} the flexural stiffness. The condition $D_{16}=D_{26}=0$ is assumed. Suppose w_0 and w_1 can be expressed as series of bi-sinusoidal functions:

$$w_0(x,y)=\sum_{m=1}^{M}\sum_{n=1}^{N}e_{mn}\sin\frac{m\pi x}{a}\sin\frac{n\pi y}{b} \quad (2)$$

$$w_1(x,y)=\sum_{m=1}^{M}\sum_{n=1}^{N}b_{mn}\sin\frac{m\pi x}{a}\sin\frac{n\pi y}{b} \quad (3)$$

where m is the half-wave number in x direction, and n the half-wave number in y direction. Substituting Eqs.(2) and (3) into Eq.(1), one obtains:

$$\left\{\pi^2[D_{11}m^4+2(D_{12}+2D_{66})m^2n^2R^2+D_{22}n^4R^4]\right\}b_{mn}$$
$$-\left\{a^2\lambda[m^2N_x+n^2R^2N_y]\right\}b_{mn}=a^2\lambda[m^2N_x+n^2R^2N_y]e_{mn} \quad (4)$$

where R is the aspect ratio of the plate, $R=a/b$. From Eq. (4),

* Supported by Hubei Key Laboratory of Roadway Bridge and Structure Engineering（2005）

we can show that the following relation holds:

$$b_{mn} = \lambda e_{mn}/(\lambda_{mn} - \lambda), \tag{5}$$

$$\lambda_{mn} \equiv \frac{\pi^2[D_{11}m^4 + 2(D_{12}+2D_{66})m^2n^2R^2 + D_{22}n^4R^4]}{a^2[m^2N_x + n^2R^2N_y]} \tag{6}$$

For a symmetric laminate, by utilizing the above relations and the lamination theory, stresses for the jth ply in the material principal directions are calculated as [4]:

$$\begin{Bmatrix}\sigma_L\\ \sigma_T\\ \sigma_S\end{Bmatrix}_j = \lambda \begin{Bmatrix}G_L\\ G_T\\ G_S\end{Bmatrix}_j + z\sum_{m=1}^{M}\sum_{n=1}^{N}\frac{\lambda e_{mn}}{\lambda_{mn}-\lambda}\times\begin{Bmatrix}H_L^{mn}(x,y)\\ H_T^{mn}(x,y)\\ H_S^{mn}(x,y)\end{Bmatrix}_j \tag{7}$$

with

$$\begin{Bmatrix}G_L\\ G_T\\ G_S\end{Bmatrix}_j = [Q][T_\varepsilon]_j [A]^{-1}\begin{Bmatrix}N_x\\ N_y\\ 0\end{Bmatrix} \tag{8}$$

$$\begin{Bmatrix}H_L^{mn}(x,y)\\ H_T^{mn}(x,y)\\ H_S^{mn}(x,y)\end{Bmatrix}_j = \left(\frac{\pi^2}{a^2}\right)[Q][T_\varepsilon]_j \times\begin{Bmatrix} m^2\sin(m\pi x/a)\sin(n\pi y/b)\\ n^2R^2\sin(m\pi x/a)\sin(n\pi y/b)\\ -2mnR\cos(m\pi x/a)\cos(n\pi y/b)\end{Bmatrix} \tag{9}$$

$$[T_\varepsilon]_j = \begin{bmatrix} c^2 & s^2 & cs\\ s^2 & c^2 & -cs\\ -2cs & 2cs & c^2-s^2\end{bmatrix}_j \tag{10}$$

$$c = \cos\theta_j,\ s = \sin\theta_j \tag{11}$$

in which $[Q]$ represents the reduced stiffness matrix, $[A]$ the tension stiffness matrix of the laminate, and θ_j the fiber angle of jth ply.

In-plane failure of the ply can generally be classified into two major failures: matrix failure and fiber breakage. For fiber breakage failure, the limit state function can be stated as [6]:

$$G_f = 1 - (F_{LL}\sigma_L^2 + F_L\sigma_L) \tag{12}$$

For matrix failure, the limit state function based on the Tsai-Wu criterion [7] is:

$$G_m = 1 - (F_{LL}\sigma_L^2 + F_{TT}\sigma_T^2 + F_{SS}\sigma_S^2 + 2F_{LT}\sigma_L^2\sigma_T^2 + F_L\sigma_L + F_T\sigma_T) \tag{13}$$

3. RELIABILITY ANALYSIS

3.1 Component Reliability

The first-order reliability method (FORM) is used to evaluate component reliability. In the reliability evaluation, the initial imperfection e_{mm} and the strength parameters X_T, X_C, , Y_T, Y_C and S are considered as the basic random variables. These basic random variables (totally m_0) are expressed as a vector $X = \{X_1, X_2, \cdots, X_{m_0}\}^T$. In FORM, X is firstly transformed to Y, the vector of equivalent uncorrelated standard normal variables. Then the component reliability index is computed as $\beta = (y^{*T} \bullet y^*)^{1/2}$ where y^* is the point on the limit state *G(Y)*=0 with minimum distance from the origin. A geometrical illustration for a limit state involving only two random variables is shown in Fig. 2. The failure probability is computed as $P(G \le 0) = \Phi(-\beta)$, where Φ is the cumulative distribution function of the standard normal variable.

In Fig.2, y^* is referred to as the design point, or the most probable failure point (MPP), which can be found using the following iterative formula:

$$y_{i+1} = \left[y_i^T\alpha_i - \frac{G(y_i)}{|\nabla G(y_i)|}\right]\alpha_I^T \tag{14}$$

where $\nabla G(y_i)$ is the gradient vector of the limit state function at y_i, and α_i is the unit vector normal to the limit state surface away from the origin.

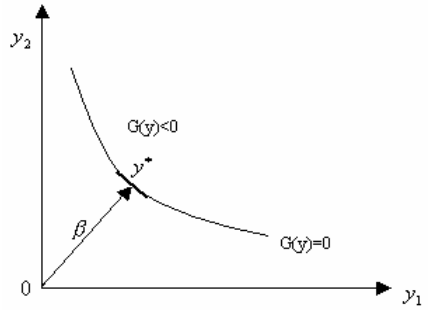


Fig.2. Geometrical illustration of the reliability index β

3.2 System Failure Probability

As mentioned earlier, a laminate can be treated as a system and ply groups as components. The failure of the laminate system may be assumed to occur using one of the two definitions: first-ply failure (FPF) and last-ply failure (LPF).

In the FPF, the failure of any of the component is defined as failure of the system. System reliability index has the following form:

$$\beta_F^s = \beta_{\min}^e \tag{15}$$

In the LPF, it is defined that the system failure can only occur when all of its components have failed. Its failure is characterized as a progressive failure, and the system failure probability is computed through the significant failure sequences, which are determined by the branch and bound technique [3].

According to this method, reliability indices of components, including matrix failure and fiber breakage in the ply-level, and the corresponding failure probabilities are computed in the first step. Next, suppose the component, which has the maximum failure probability $P_{f\max}^1$, fails. If the event is corresponding to matrix failure, this ply's modulus E_2 and G_{12} will be reduced to zero. If the event is corresponding to fiber failure, this ply's modulus E_1 will be reduced to zero. The laminate stiffness is modified and computation is repeated. This proceeds are repeated until the system failure occurs. The significant failure sequence is thus identified.

The system failure probability P_f (or system reliability index β_L^s) may be evaluated by the failure sequence. And the second-order upper bound method is used to estimate the failure probability of the significant failure sequence. Noting that a failure sequence is a parallel system and suppose there are *m* events in the sequence, then

$$P_f = P(\cap_{j=1}^m E_j) \le \min_{i\ne j}(P(E_i \cap E_j)) \tag{16a}$$

$$P(E_i \cap E_j) = \Phi(-\beta_i, -\beta_j, \rho_{ij}) \tag{16b}$$

where E_j is the *j* th basic failure event in the failure sequence under the condition that the first (*j*-1) basic failure events have occurred, Φ is the bi-normal distribution function, β_i,

β_j are reliability indices, and ρ_{ij} is the correlation coefficient computed as

$$\rho_{ij} = \sum_{r=1}^{m_0} \alpha_{ir}\alpha_{jr} \tag{17}$$

where m_0 is the number of basic random variables, α_{ir} and α_{jr} are the components of the unit gradient vectors of the limit states i and j, respectively (Fig.3).

For nonlinear problems, the two limit state functions are linearized with respect to their intersection, which is found from the constrained minimization problem:

$$\text{Minimize } \sqrt{Y^T Y}, \quad \text{s.t. } G_i(Y)=0;\ G_j(Y)=0 \tag{18}$$

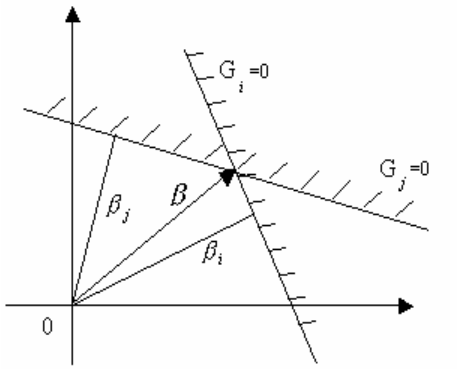


Fig.3. Two intersecting tangent plane

4. RELIABILITY-BASED OPTIMUM

An optimization problem has three components: (1) objective function; (2) constraints; (3) algorithms. In this paper, the reliability-based optimum design is to use the system reliability index as the objective function, the fiber orientation and the lamina thickness as the design variables. Genetic algorithm is used to search for the optimum solutions. The optimum problems are expressed in the example.

For the optimum design, we seek an adequate value of the design variable, which satisfies the constrained condition and makes the objective function minimum, namely to seek the optimum solution.

Table l Loading conditions and the mechanical properties

	Units	Value
Nx	KN/m	600
E_1	GPa	181.0
E_2	GPa	10.7
G_{12}	GPa	7.17
ν	--	0.28

Table 2 Random variables

	Units	Mean	Standard Deviation	Distribution Type
e_{11}	mm	0	0.6	Normal
e_{21}	mm	0	0.06	Normal
e_{31}	mm	0	0.02	Normal
e_{41}	mm	0	0.006	Normal
X_T	MPa	1500	150	Normal
X_C	MPa	1500	150	Normal
Y_T	MPa	40	4	Normal
X_C	MPa	246	24.6	Normal
S	MPa	68	6.8	Normal

5. NUMERICAL EXAMPLES

As shown in Fig.1, a simply supported symmetric laminated plate subjected to a bi-axis compression load N_x and N_y, a load ratio is defined to be $k = N_y / N_x$, $a \times b$=20×12.5 cm^2. The stacking sequence is $[45_n(+\theta)_m(-\theta)_{12-m-2n}(-45)_n]_s$, the thickness of the 45^o, -45^o ply is n × h_0, $+\theta^o$ ply is m× h_0, $-\theta^o$ ply is (10- m-n)× h_0, h_0=0.1mm, and the total thickness is 24× h_0=2.4mm. The composite material is a typical graphite/epoxy (T300/5208). The loading conditions and the mechanical properties of the material are listed in Table 1. The statistical characteristics for the initial imperfection (m=1,2,3,4; n=1), and strength parameters are given in Table 2. All the random variables are assumed to be normally distributed variables, for the sake of illustration. It is assumed that these random variables are uncorrelated.

Denote the system reliability index as β^s (β_F^s is that based on the FPF, and β_L^s the LPF). Consider the optimum problem as follows

$$\text{Minimize } f(\theta,m) = -\beta^s \text{ (or Maximize } \beta^s) \tag{19}$$

$$\text{Subject: } 0 \le \theta \le 90, 1 \le m \le 7$$

Where θ、m are the design variables, and n=2.

Firstly to demonstrate the validity of the Genetic algorithm, consider the system reliability based on the FPF criterion. One is optimized by genetic algorithm, and the other is done by the sequence quadratic programming (SQP) method. The results are compared in Table 3. It shows that the optimum solutions with two different algorithms are very closely, which confirms that the genetic algorithm to be effective.

Table 3. The optimum solutions with two different algorithms

k	Genetic algorithm			SQP		
	$\theta_{/(^0)}$	m	β	$\theta_{/(^0)}$	m	β
1.0	48.2	4	0.542	48.2	4	0.545
0.8	42.5	4	0.798	42.6	4	0.787
0.6	40.1	3	1.108	40.1	3	1.104
0.4	38.5	4	1.420	38.4	4	1.427
0.2	25.7	4	1.986	25.7	4	1.976
0.0	0	3	2.559	0	4	2.560

Now to optimize the problem (19), the system reliability indices are computed in two cases, one is in the FPF and the other is the LPF. The optimum solutions are showed in Fig.4 and Table 4.

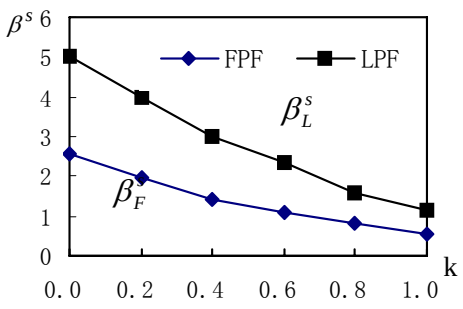


Fig.4. The optimum reliability indices-k relations

Fig 4 shows that, as the load ratio k increase form 0 to 1.0, the system reliability indices are decreased in both of the two cases. When k=0, β_F^s =2.559, β_L^s =5.021,and when k=1.0, β_F^s =0.542, β_L^s =1.123. The difference of two cases as k=0 is larger than that as k=1.0. It shows that the objective β_L^s is larger than β_F^s while k=0 to k=1.0. So it shows that optimum design based on the LPF is taken full advantage of the material behavior than the FPF.

Table 4. the optimum solutions of FPF and LPF

k	FPF		LPF	
	θ /(0)	m	θ /(0)	m
1.0	48.2	4	46.1	4
0.8	42.5	4	40.6	4
0.6	40.1	3	39.6	4
0.4	38.5	4	29.6	4
0.2	25.7	4	15.5	4
0.0	0	3	0	3

Table 4 shows the optimum ply numbers m are close as k takes different values. But the optimum fiber orientations θ are different as k takes from 0 to 1.0, when k=0, for the two cases θ are same, equal 0, and as k takes other values, θ of FPF is larger than that of LPF.

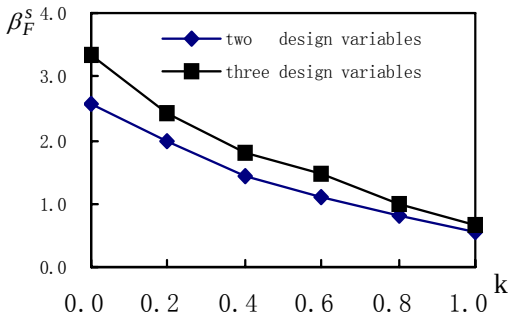


Fig.5. The optimum reliability indices-k relations of FPF

If we take the ply number n as the design variable, so the design variables are three: θ、m、n. Figure 5 and Table 5 show the optimum solutions based on the FPF. Fig 5 shows that the system reliability indices decrease as k takes from 0 to 1.0. as k takes from 0.0 to 1.0, β_F^s optimized with two design variables are larger than that with three. Table 5 indicates the optimum solutions for the two cases are much different.

Table 5. the optimum solutions of FPF

k	Two design variables			Three design variables		
	θ /(0)	m	n	θ /(0)	m	n
1.0	48.2	4	2	52.1	4	3
0.8	42.5	4	2	48.5	3	3
0.6	40.1	3	2	41.8	3	3
0.4	38.5	4	2	29.2	3	3
0.2	25.7	4	2	0	5	2
0.0	0	3	2	0	7	2

Fig 6 and Table 6 express the optimum results based on the LPF. From Fig. 6 we can see that the β_L^s optimized with three design variables are almost equivalent that with two. Table 6 shows that the optimum orientations with two design variables are less than that with three design variables.

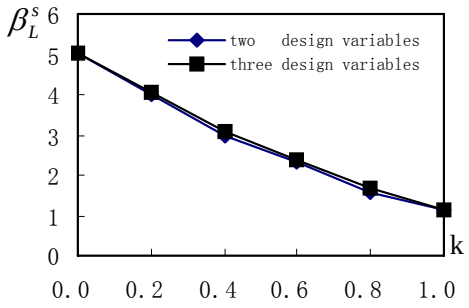


Fig.6. The optimum reliability indices-k relations of LPF

Table 6 the optimum solutions of LPF

k	Two design variables			Three design variables		
	θ /(0)	m	n	θ /(0)	m	n
1.0	46.1	4	2	46.1	4	2
0.8	40.6	4	2	36.1	3	3
0.6	39.6	4	2	26.9	3	3
0.4	29.6	4	2	25.2	3	3
0.2	15.5	4	2	10.2	4	3
0.0	0	3	2	0	3	2

6. CONCLUSIONS

In this paper, we first developed a method to evaluate the system reliability of laminated composites. Then an optimum design problem is formulated and solved.

Since properties of the constitutes may differ from the nominal ones owing to statistical variations, and the geometry of a real structure will be different from the design because of the manufacturing error, etc. the reliability-based optimum design can be very impartment in practice. The optimal solutions based on the LPF are compared with those on the FPF, And the optimum design based on the LPF takes full advantage of the material property than the FPF. Numerical examples are given to show the necessity and the advantage of the reliability-based optimum design.

REFERENCES

[1] Park.W.J, “An optimal design of simple symmetric laminates under the first ply failure criterion”, *Journal of Composite Materials*, 1982,16: 341-355

[2] S.Mahadevan and X.Liu, “Probabilistic optimum design of composite laminates”, *Journal of Composite Materials*, 1998,32: 68-82

[3] S. Mahadevan, X. Liu and Q. Xiao, “A probabilistic progressive failure model of compositelaminates”, *Journal of Reinforced Plastics and Composites*, 1997,16, 1020-1038

[4] Chen Jianqiao, Wang Xiangyang and Luo Cheng, “Reliability analysis of FRP laminated plates with consideration of both initial imperfection and failure sequence”, *Acta Mechanica Solida Sinica*, 2002,15(3): 227-235

[5] N. Kogiso and Y. Murotsu, “Reliability analysis of Laminated composite plate with initial imperfection”. *Trans JSME, Ser.A*, 2000,66:1483-1490

[6] Tan.S.C, “A progressive failure model for composite laminates containing openings”, Journal of Composite Materials, 1991,25:557-577

[7] S.W.Tsai and H.T.hahn, “Introduction to Composites Materials”, *Technomic Publishing Co*., Inc., Lancaster, PA, 1980

Xiangyang Wang is an associate Professor in School of Transportation, Wuhan University of Technology. He graduated from Huazhong University of Science and Technology in 2004 with specialty of solid mechanics, and has acquired the Ph.D degree. He has published over 20 Journal papers. His research interests are in bridge structures, composite materials mechanics.

A New Parallel Algorithm for Finding Convex Hull Based on COW with 2-Clusters, 2-Domains and 2-Directions

Qihai Zhou , Hongyu Wu
School of Economic Information Engineering, Southwestern University of Finance and Economics
Chengdu, Sichuan 610074, China
Email: zhouqh@swufe.edu.cn

ABSTRACT

This paper comment on the lower efficiency shortcomings of representative both series algorithms for finding convex hull (for example: Gift wrapping convex hull algorithm, Graham scan convex hull algorithm, and Algorithm for finding convex hull based on coiling with a minimum lever pitch) and parallel algorithms for finding convex hull(for example: Half-dividing convex hull algorithm, Rapid convex hull algorithm ,Grid convex hull algorithm),and based on the isomorphic fundamental theorem of the convex hull construction, a more efficient new parallel algorithm to find a convex hull based on COW is given. The general characters of the new algorithm are: 1) its COW is combined with two sub-clusters; 2) its domain sub is divided into two sub-domains; 3) its seeking direction is along with two ways (i. e. clockwise direction, and anti clockwise direction).

Keywords: Isomorphic, COW, Convex Hull, Parallel Algorithm, Two Sub-Clusters, Two Sub-Domains, Two Ways

1. INTRODUCTION

Since the 20th century 70's, the 2D Convex Hull problem's complexity and its application importance had caused the domestic and foreign experts quite to pay attention to the convex hull algorithms, and many documents explain the important meaning of researching, improving and enhancing the efficiency of the algorithm of 2D point set and line segment set. Up to the present, there are a lot of series algorithms for finding convex hull (for example: Gift wrapping convex hull algorithm, Graham scan convex hull algorithm, Algorithm for finding convex hull based on coiling with a minimum lever pitch in single domain and single direction) [1-4] ,and parallel algorithms for finding convex hull (for example: Half-dividing convex hull algorithm, Rapid convex hull algorithm ,Grid convex hull algorithm)[4-8]. But these parallel algorithms based on series algorithm, and they use recursion, so the efficiency is not high. Then a new more efficient algorithm to find a convex hull based on COW (abr. from Cluster Of Workstation) is given by us according to the isomorphic fundamental theorem of the convex hull construction.

2. THE DESCRIPTIONS OF THE PROBLEM OF 2D CONVEX HULL AND THE CONVEX HULL ALGORITHM

DEFINITION 1: Suppose that Q is the polygon in given plane, $Q_1(x_1, y_1)$, $Q_2(x_2, y_2)$, …, $Q_n(x_n, y_n)$ are the spots of Q. If any line segment Q_iQ_j ($i \neq j$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n < +\infty$) is all not outside Q, then Q is called a convex polygon.

DEFINITION 2: Suppose that the 2D point set $S=\{P_i(x_i,y_i) \mid 1 \leqslant i \leqslant m, 3 \leqslant m < +\infty\}$ is composed by the spots which are in the given plane. If the apexes of polygon Q belong to S, and Q is the least Convex Polygon which covers all points in S, then Q is called the convex hull of the 2D point set S.

DEFINITION 3: How to seek the convex hull of the given 2D point set $S=\{P_i(x_i,y_i) \mid 1 \leqslant i \leqslant m, 3 \leqslant m < +\infty\}$ is called 2D Convex Hull problem.

DEFINITION 4: An algorithm which could produce 2D convex hull of the given 2D point set is called 2D Convex Hull algorithm.

3. THE SUMMARY OF PARALLEL ALGORITHM

The method of parallel program is different from the method of series program, and the difference is the attitude to the problem: the method of series program regards the change of affair as single-track. Any two of the affair may exist causality, and then regards a series of correlative affair as an inseparable whole. To the cognition of affair, structure programming especially the object programming make breaking evolvement (namely: they decompose a complicated affair to many simple affairs, indeed regards a system as composed by many relative entities); but both with a view to the affair's the relation of static state construction and the action's pattern of surface layer, and had not achieve that cognize and decompose affair from the relation of dynamic state construction and the action's pattern of deep seated. As a result, from the essence of action mode, the affair is taken for coherent or one after the other, it doesn't exist the phenomenon of subsequent interfere, and doesn't exist coincidental actions which happen at the same time. The basic viewpoint of the method of parallel programming is taken the action of one affair as the result of reciprocity of many sub-affairs (series or parallel). This is the fundamental change of conception of programming. The core method of parallel programming which it leads is the affair's parallel partition and algorithm mapping. The foundation of exoteric is the module of parallel computing. The module of parallel computing decides the semanteme of parallel, the semanteme of parallel decides the rule of parallel executing, consequently decides the principle of parallel partition.

DEFINITION 5: Parallel algorithm is an aggregation of many courses which could finish the problem at the same time with reciprocity, harmony, uniformity, and consensus.

DEFINITION 6: The parallel algorithms which adopt the method of synchronization (the execution of all algorithm's threads must wait each other), the method of asynchronization (the execution of all algorithm's threads could not wait each other), the method of distribution (many sizes or nodes which are connected by corresponding link finish the problem) are called synchronized algorithm, asynchronized algorithm, distributed algorithm respectively.

According to the universality and dominating of distributed algorithm, so the implementing method of parallel convex hull algorithm which is discussed in this paper adopts distributed convex hull algorithm.

4. THE SYNOPSIS OF THE CLUSTER OF WORKSTATION

The cluster of workstation is called COW for short. It connects a set of high-powered workstation according to topological structure by high speed universal net, and with the help of parallel programming and the compositive exploitation's environment of man-machine alternation which is viewed, we attempter unitive, dispose harmonious and implement high-efficiency high-powered computation's parallel system. Every node of COW has integrated operating system. From the view of system's structure and the way of communications between nodes, COW is the part of distributed storable MIMD's parallel computer structure. It implements the correspondence among each of host computers by the way of information impressing. The environment of parallel programming which is based on commonly operating system has finished the system's management of resource and collaboration each other. At the same time it shields the isomerism of workstation and net. So to programmers and users, the system of COW is a unitary system of parallel management. The host computer and net which are in the system of COW may be isomorphic or isomeric. The general system structure of COW is shown as Fig. 1.

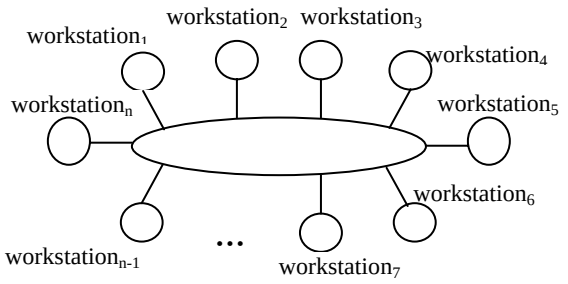


Fig. 1. The sketch map of the cow's structure of system

In the system of the COW, each of the workstations has its own memory and I/O equipment, its structure as shown in Fig. 2.

The characteristics of the system of COW are:

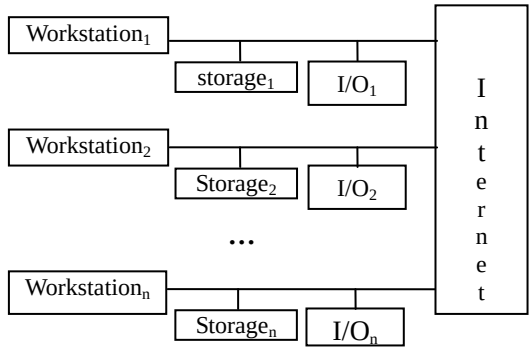


Fig. 2 . The sketch map of basic structure of a workstation of COW

1) The adoption of environment is strong, and the period of development is short. The emphases of development is communication and the environment of parallel programming, it needn't to research nodes over again, and needn't to design operating system and compiled system, so it saves a great deal of time.
2) The robust of system is good and the risk of investment is little. The system of COW is not only a parallel system, every node of it is also an absolute workstation, even though the parallel efficiency of the whole system is not high, but the node of it is still a workstation.
3) The ratio between property and price is good and the development of system's cost is low. Because of the little batch, the cost of traditional huge computer or MPP is high, and the price is high (millions to multimillions dollars at every turn). But the workstation belongs to volume-produce, so the cost and price is low much.
4) The utility ratio of system is high and it saves the resource; it could use existing equipment plenitudinously, so only see from the utility ratio, the utility of the system of COW is much higher than the utility of the system of stand-alone.
5) The ductibility of system is good and the expansibility of system is strong. From the scale, the system of COW almost uses general net. The expansibility of system is easy. From the capability, the parallel application of most middle or coarse granularity has high efficiency.
6) The ratio of repeating is high and the whip of programming is concise. In the system of COW, the parallel of program always insert corresponding communicating language, and we make little modification to the resource base of series program.

Therefore, this paper adopts the COW to research and implement the parallel of convex hull algorithms.

5. A NEW PARALLEL ALGORITHM FOR FINDING CONVEX HULL BASED ON COW WITH 2-CLUSTERS, 2-DOMAINS AND 2-DERECTIONS

DEFINITION 7: The distributed domain of every point in 2D point set S={Pi(xi,yi)｜ 1≤i≤m, 3≤m<+∞} is called the S distributed domain.

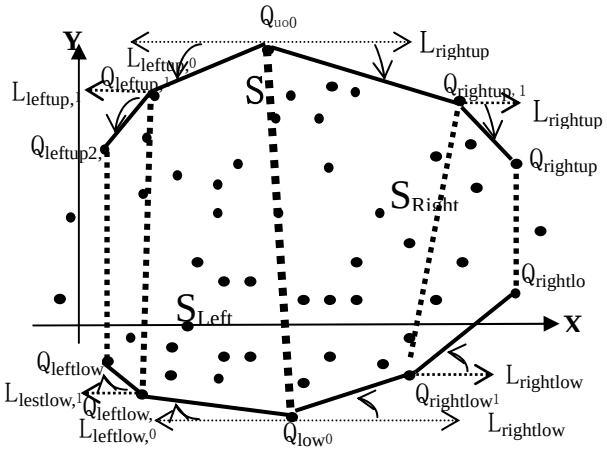


Fig. 3. The sketch map of initial Poles and sub-domains of convex hull

DEFINITION 8: In 2D point set S={$P_i(x_i,y_i)$｜1≤i≤m, 3 ≤ m<+ ∞ },the outside-most points which have the

maximum or minimum y-coordinate are recorded: $P_{(1)}(x_1, y_1=\min\{y_i\ (1\leqslant i\leqslant m\geqslant 3)\})$, $P_{(2)}(x_2, y_2=\max\{y_i\ (1\leqslant i\leqslant m\geqslant 3)\})$; The outside-most points $P_{(1)}$, $P_{(2)}$are called initial poles of convex hull Q and recorded as Q_{up0},Q_{low0} (it means: Q_{up0} is the right high initial poles of sub-domain S_{right},S_{left}; as the same as Q_{low0}). The line segment $Q_{up0}Q_{low0}$ is called the line of demarcation of the convex hull (called baseline for short). The line of demarcation divide the original distributed domain into two sub-domains which are sub-domains S_{right},S_{left} called as sub-domains of 2D point set (shown as in Fig 3).

DEFINITION 9: Do not loose universality, in 2D point set $S=\{P_i(x_i,y_i) \mid 1\leqslant i\leqslant m\geqslant 3\}$,the initial poles of convex hull Q are Q_{up0},Q_{low0}, and they are also recorded as $Q_{rightup,0}$,$Q_{rightlow,0}$ or $Q_{leftup,0}$, $Q_{leftlow,0}$. In the sub-domain of S, S_{right} make radials $Q_{\ rightlow,j}L_{\ rightlow,j}$ and $Q_{\ rightup,j}L_{\ rightup,j}$ which across the current new poles $Q_{rightlow,j}$,$Q_{rightup,j}$ ($0\leqslant j\leqslant$ mright） of the sub-convex hull Q_{Right} respectively, and parallel the positive direction of X-axes. The radials are called positive radials. The angles $\angle P_iQ_{rightlow,j}L_{rightlow,j}$,$\angle P_iQ_{rightup,j}L_{rightup,j}$ which is formed by positive radials $Q_{rightlow,j}L_{rightlow,j}$,$Q_{rightup,j}L_{rightup,j}$ which are coiled to the point $P_j(x_j,y_j)\in S$ according to anticlockwise (that is called A direction for short), clockwise(that is called B direction for short) are called the A direction angle of the point $P_j(x_j,y_j)$ to positive radial $Q_{rightlow,j}L_{rightlow,j}$,and B direction angle of the point $P_j(x_j,y_j)$ to positive radial $Q_{rightup,j}L_{rightup,j}$.

The first author points out the isomorphic direction of the convex hull algorithm's improvement and optimizing. In document [3~6], the improvement to document [2] is clarified (where: document [5] is the improvement of document [3~4]). On the basis of document [5], the paper brings forward a new parallel algorithm for finding convex hull based on COW with 2-clusters (it means the COW is divided into two sub-COWs), 2-domains (it means the domain is divided into two sub-domains) and 2-directions (it means the direction for finding the poles of convex hull is divided into clockwise and anticlockwise). The algorithm's thought may be structured as follows:

Step 0: Parallel Initialization Processing.

(1) 2-clusters parallel processing of "finding the maximum and minimum of y-coordinate in domain S":

1) Record the two sub-clusters as COW_{right},COW_{left}, and record the sum of the processor which is belonged to sub-clusters COW_{right},COW_{lef} as n_{right},n_{left}. Record the processor which is belonged to sub-clusters COW_{right},COW_{left} as $P_{right\ j}(1\leqslant j\leqslant n_{right})$, $P_{left\ k}(1\leqslant k\leqslant n_{left})$. Suppose the maximum and minimum of X-coordinate are x_{max},x_{min} in initializing domain $S=\{P_i(x_i,y_i) \mid 1\leqslant i\leqslant m\geqslant 3\}$.
2) Every processor $P_{right\ j}(1\leqslant j\leqslant n_{right})$ which is belonged to sub-cluster COW_{right} make the zonal partition according to the initial bandwidth $W_{S\ width}(=(x_{max}-x_{min})/(n_{left}+n_{right}))$, if the initial domain is not null, then find out two outmost points of the maximum and minimum of y-coordinate of $S_{right,initial\ j}$, and find out two outmost points of the maximum and minimum of y-coordinate in right sub-domain $S_{right\ initial}$ which is composed by each of $S_{right\ initial\ j}$ from all outmost points of initial domain $S_{right\ initial\ j}$.
3) Every processor $P_{left\ j}(1\leqslant j\leqslant n_{left})$ which is belonged to sub-cluster COW_{left} make the zonal partition according to the initial bandwidth $W_{S\ width}(=(x_{max}-x_{min})/(n_{left}+n_{right}))$, if the initial domain is not null, then find out two outmost points of the maximum and minimum of y-coordinate of $S_{left\ initialj}$, and find out two outmost points of the maximum and minimum of y-coordinate in left sub-domain $S_{left\ initial}$ which is composed by each of $S_{left\ initial\ j}$ from all outmost points of initial domain $S_{left\ initial\ j}$.
4) As the sub COW(shown as in Fig 3), both COW_{right} and COW_{right} find out two outmost points of the maximum and minimum of y-coordinate of initial domain S among the four outmost points of the maximum and minimum of y-coordinate of right sub-domain $S_{right\ initial}$ and left sub-domain $S_{left\ initial}$; and recorded $P_{(1)}(x_1,y_1=\max\{y_i\ (1\leqslant i\leqslant m\geqslant 3)\})$, $P_{(2)}(x_2, y_2=\min\{y_i\ (1\leqslant i\leqslant m\geqslant 3)\})$. The outmost points $P_{(1)}$,$P_{(2)}$ are the initial points of convex hull Q of S, and recorded Q_{up0},Q_{low0}.

(2) The 2-cluster parallel processing of conforming two sub-domains of domain S:

1) Connect the initial points Q_{up0},Q_{low0} in order to create the dividing baseline in the sub-COW COW_{right},COW_{left} respectively. The baseline could plot the two sub-domain S_{right},S of the domain of 2D point set, which is disposed later.
2) Choose and hold the points' data of sub-domain S_{right}, S_{left} in the sub-COW COW_{right}, COW_{left} respectively. Work out the bandwidth of sub-domain $S_{right\ j}$ ($1\leqslant j\leqslant n_{right}$), S_{left} ($1\leqslant j\leqslant n_{left}$) $W_{right\ width}=(\max\{x_i \mid x_i\in S_{right}\}-\min\{x_i \mid x_i\in S_{right}\})/\ n_{right}$,$W_{left\ width}=(\max\{x_i \mid x_i\in S_{left}\}-\min\{x_i \mid x_i\in S_{left}\})/\ n_{left}$.
3) Every processor $P_{right\ j}$ ($1\leqslant j\leqslant n_{right}$), $P_{left\ k}$ ($1\leqslant k\leqslant n_{left}$) which is belonged to sub-cluster COW_{right} and COW_{left} divide the initial domain S into sub-domain $S_{right\ j}$ ($1\leqslant j\leqslant n_{right}$), $S_{left\ k}$ ($1\leqslant k\leqslant n_{left}$) according to the bandwidth $W_{right\ width}$, $W_{left\ width}$. The sub-COW COW_{right} and COW_{left} prepare the points which are decided by the sub-domains S_{right}, S_{left} and except the initial points Q_{up0}, Q_{low0}.

Step 1: The parallel processing of sub-COW COW_{right} and COW_{left} generate the vertexes of sub-convex hull Q_{right}, Q_{left} in the sub-domains S_{right}, S_{left}.

Step 1-1: The parallel processing of the sub-COW_{right} finding the vertexes of sub-convex hull Q_{right} based on coiling with a minimum lever pitch in double direction in the sub-domain S_{right}.

Step 1-1-1: The parallel processing of the sub-COW_{right} finding the next couple of new vertexes of sub-convex hull Q_{right} based on coiling in double direction in the sub-domain S_{right}.

Step 1-1-1-1: Record the initial domain S_{right} as the current sub-domain S_{right}, record the initial vertexes Q_{up0}, Q_{low0} as the new couple of vertexes $Q_{right\ up}$, $Q_{right\ low}$. Set r be 0.

Step 1-1-1-2: Every processor $P_{right\ j}$ ($1\leqslant j\leqslant n_{right}$) which is belonged to sub-cluster COW_{right} divide the initial domain S into sub-domain $S_{right\ j}$ ($1\leqslant j\leqslant n_{right}$) according to the bandwidth W_{right}.

Step 1-1-1-3: Every processor $P_{right\ j}$ ($1\leqslant j\leqslant n_{right}$) which is belonged to sub-cluster COW_{right} work out the least points $P_{right\ j\ A}$, $P_{right\ j\ B}$ based on coiling with a minimum lever pitch in double direction of A-direction

and B-direction in their own sub-domain $S_{right\ j}$ ($1 \leqslant j \leqslant n_{right}$) respectively. Find out the least points $P_{right\ A}$, $P_{right\ B}$ of A-direction and B-direction among the least points $P_{right\ j\ A}$, $P_{right\ j\ B}$ ($1 \leqslant j \leqslant n_{right}$) of A-direction and B-direction. Set r be r+1, and regard $P_{right\ A}$, $P_{right\ B}$ as the next couple of vertexes $Q_{right\ up,r}$ and $Q_{right\ low,\ r}$ of sub-convex hull Q_{right}.

Step 1-1-2: The process of deleting the points of the sub-convex hull $Q_{right\ up,r-1}Q_{right\ low,r-1}Q_{right\ low,r}$ $Q_{right\ up,r}$, which is composed by the couple of vertexes $Q_{right\ up,r-1}$, $Q_{right\ low,r-1}$ and the couple of vertexes $Q_{right\ up,r}$, $Q_{right\ low,r}$.

Step 1-1-2-1: If the fresh couple of vertexes $Q_{right\ up,\ r}$, $Q_{right\ low,\ r}$ is different,

Then: every processor $P_{right\ j}$ ($1 \leqslant j \leqslant$ nright) which are belonged to sub-cluster COW_{right} divides the domain Q into sub-domains QQ_{rightj} ($1 \leqslant j \leqslant n_{right}$) where the sub-convex hull $Q_{right\ up,\ r-1}Q_{rightlow,r-1}Q_{rightlow\ ,\ r}Q_{rightup,r}$ located with the bandwidth $W_{right\ width}$=(max{x_i | x_i is the point in sub-convex hull $Q_{right\ up,r-1}Q_{right\ low,r-1}Q_{right\ low,r}$ $Q_{right\ up,r}$}-min{x_i | x_i is the point in sub-convex hull $Q_{right\ up,r-1}Q_{right\ low,r-1}Q_{right\ low,r}$ $Q_{right\ up,r}$ })/n_{right}.

Otherwise: switch to execute Step 1-1-3.

Step 1-1-2-2: Every processor $P_{right\ j}$ ($1 \leqslant j \leqslant n_{right}$) which are belonged to sub-cluster COW_{right} delete all points of own sub-domain $QQ_{right\ j}$ ($1 \leqslant j \leqslant n_{right}$).

Step 1-1-2-3: Record the primary sub-domain S_{right} which is deleted all the points in QQ_{right} as the current sub-domain S_{right}.

Step 1-1-3: The process of all vertexes signing in sub-convex hull Q_{right}: sign all the vertexes of convex hull Q_{right} which have been worked out.

Step 1-2: The same to Step 1-1, the parallel processing of the sub-COW_{left} finding the vertexes of sub-convex hull Q_{left} based on coiling with a minimum lever pitch in double direction in the sub-domain S left.

Step 1-2-1: The parallel processing of the sub-COW_{left} finding the next couple of new vertexes of sub-convex hull Q_{left} based on coiling in double direction.

Step 1-2-2: The process of deleting the points of the sub-convex hull $Q_{left\ up,r-1}Q_{left\ low,r-1}Q_{left\ low,r}$ $Q_{left\ up,r}$, which is composed by the couple of vertexes $Q_{left\ up,r-1}$,$Q_{left\ low,r-1}$ and the couple of vertexes $Q_{left\ up,r}$, $Q_{left\ low,r}$.

Step 1-2-3: The process of all vertexes signing in sub-convex hull Q_{left}: sign all the vertexes of convex hull Q_{leftt} which have been worked out. (Annotation: the principle, method, step and operation of Step 1-1, Step 1-1-1, Step 1-1-2 and Step 1-1-3 are same. So change the "right, left, A-direction, B-direction" of Step 1-1 into "left, right, B-direction, A-direction" of Step 1-2, and the operation of Step 1-2, Step 1-2-1, Step 1-2-2 and Step 1-2-3 are omitted.)

Step 2: The process of fit together the vertexes of sub-convex hull Q_{right}t, Q_{left} which are gained by sub-COW COW_{right}, COW_{left}. Namely: the convex polygon Q which is composed by the line segments which link the apexes orderly in sub-convex hulls Q_{right}, Q_{left} must be the convex hull Q in 2D limited point set S.

6. CONCLUSIONS

The algorithm that is proposed in this paper not only in the running time and space complexity but also in the efficiency, obviously surpasses the Gift wrapping convex hull algorithm, Graham scan convex hull algorithm, Half-dividing convex hull algorithm and so on. Moreover, it is very easy to be transformed into new parallel algorithm for finding convex hull based on COW with m-Clusters, n-Domains and p-Directions where m>2, n>2, p>2 (we shall discuss them in other papers). Therefore, it will enhance the speed of constructing 2D convex hull effectively, and could improve and enhance the application level and the working efficiency of the 2D convex hull in the imagery processing, the writing decomposes, the pattern recognition, the object classification, the computation graph, the fingerprint recognition, the telemeter remote control, the thing recognizes, the geological prospecting, the space & sky using, and so on.

REFERENCES

[1] Zhou Qihai, "the direction of improving algorithm of

[2] onvex Hull in 2D points set or line set"[J],*The computer science*,2007.

[3] Zhou Qihai,Yang, Xiangmao,Wu Hongyu. "A New Algorithm for Finding Convex Hull Based on Coiling with a Minimum Lever Pitch in Single Domain and Single Direction"[J],*Journal of XiHua University Natural Science Edition*,2006

[4] Zhou Qihai,Wu Hongyu,Huang Tao,"A New Algorithm for Finding Convex Hull Based on Coiling with a Minimum Lever Pitch in Single Domain and Double Direction,"[J]. *The computer science*,2007.

[5] Zhou Qihai,Huang Tao,"A New Algorithm for Finding Convex Hull Based on Coiling with a Minimum Lever Pitch in Double Domain and Single Direction,"*The Collection of 13th National Conference on Image and Graphics*,2007.

[6] Zhou Qihai,Wu Hongyu,"A New Algorithm for Finding Convex Hull Based on Coiling with a Minimum Lever Pitch in Double Domain and Double Direction,"*The Collection of 13th National Conference on Image and Graphics*,2007.

[7] Zhou Qihai,Huang Tao,Wu Hongyu,Zhang Yuanxin, "Maximum Pitch of the Dynamical Basic Line Convex Hull Algorithm,"[J]. *The computer science* ,2007.

[8] Zhou Qihai,"The condition and development of Convex Hull in 2_D Points,"*The Collection of 13th National Conference on Image and Graphics*,2007.

[9] Chen Guoliang. *Parallel computation structure algorithm programming*,[M].Higher education publishing house, 2,002 years.

[10] Zhou Peide,*Computation geometry algorithmic analysis and design*,[M].Qinghua University publishing house, 2,000 years.

[11] Greg Aloupis,"A History of Linear-time Convex Hull Algorithms for Simple Polygons,"[J]. Http://En.Wikilib.Com / Wiki/Talk:Convex_hull.

[12] Dan Sunday,"The Convex Hull of a 2D Point Set or Polygon" [J]. Http://Softsurfer.com/Archive/Algorithm_01 09 / Algorithm_0109.Htm

[13] Joseph O'Rourke,*Computational Geometry in C* (2nd Edition), Chap. 3 "Convex Hulls in 2D" [M] (1,998).
[14] C. Barber,D. Dobkin,And H. Huhdanpaa,“The Quickhull algorithm for convex hulls,”[J].*ACM Trans,On Mathematical Software*,22,pp.469-483,1997.
[15] D.G. Kirkpatrick & R. Seidel,“The Ultimate Planar Convex Hull Algorithm,”[J].*SIAM Jour. Comput*,15, pp.287-299 (1,986)
[16] Franco Preparata & Michael Shamos,Computational Geometry:An Introduction,Chap. 3,"Convex Hulls: Basic Algorithms "[M],(1,985).
[17] M. Kallay,“The Complexity of Incremental Convex Hull Algorithms in Rd,”[J].*Info. Proc. Letters* 19,197(1,984).
[18] A.M. Andrew,"Another Efficient Algorithm for Convex Hulls in Two Dimensions,"[J].*Info.Proc.Letters* 9, pp.216-219(1,979).
[19] S.G. Akl & Godfried Toussaint,"Efficient Convex Hull Algorithms for Pattern Recognition Applications,"[J],in *Proc. 4th Int'l Joint Conf. On Pattern Recognition* [M].Kyoto,Japan,pp.483-487 (1,978).
[20] A. Bykat,“Convex Hull of a Finite Set of Points in Two Dimensions”[J].*Info. Proc. Letters* 7,pp.296-298(1,978).
[21] Franco Preparata & S.J. Hong,“Convex Hulls of Finite Sets of Points in Two and Three Dimensions”[J],*Comm. ACM* 20,pp.87-93(1,977).
[22] W. Eddy,“A New Convex Hull Algorithm for Planar Sets,”[J].*ACM Trans. Math. Software* 3 (4),pp.398-403 (1,977).
[23] R.A. Jarvis,“On the Identification of the Convex Hull of of a Finite Set of Points in the Plane,”[J].Info.Proc. Letters 2,pp.18-21,(1,973).
[24] Ronald Graham,“An Efficient Algorithm for Determining the Convex Hull of a Finite Point Set,”[J].Info.Proc. Letters 1,pp.132-133,(1,972).
[25] D. Chand and S. Kapur,“An algorithm for convex polytopes”[J],*ACM*,17,pp.78-86,1970.

Qihai Zhou is a Full Professor, Doctor’s tutor and a head of Information Technology and Application Institute in School of Economic Information Engineering, Southwestern University of Finance and Economics. He graduated from Lanzhou University, China in 1982; is one of “The one hundred academic and managerial leading heads of China informationalization”. He has published more than 40 books, over 160 papers. His research interests are in computational geometry, algorithm study, economics & management computation, and so on.

Parallel Multi-Grid Algorithm and Its Performance of Fluent Software*

Jianghong Yu [1], Jinsheng Xiao [1, 2], Zongbo Zhu [1, 3], Feng Ye [1, 2]
[1]The State Key Laboratory of Advanced Technology for Materials Synthesis and Processing
[2]School of Automotive Engineering, [3]Center of Modern Education Technology
Wuhan University of Technology, Hubei 430070, China
Email: [1]jhyu_07_02@163.com, [2]jsxiao@whut.edu.cn

ABSTRACT

The Fluent software is a popular CFD software package now, it can use parallel multi-grid method to solve the large-scale problems. In order to find out the suitable scale and parallel granularity of the Fluent software while it makes the solution, and make the best of the software and the hardware, this article analyses the multi-grid method and domain decomposition method of the Fluent software and tests again and again. This article mainly discusses the influence of the different multi-grid cycle method, domain decomposition method, the scale of sample and the number of computing nodes on parallel efficiency. The results from the theories analysis and the experiments show that the Fluent software has favorable parallel performance and the PEM Fuel Cell Model and HPCC could have better performance by upgraded well.

Keywords: Fuel Cell, Multi-grid, Domain Decomposition, Parallel Computing, Fluent

The Fluent software is a CFD (Computational Fluid Dynamics) solver, which can solve all kinds of complex flows, including incompressible flow (low subsonic), to weak compressible flow (transonic) and strong compressible problems (supersonic), Fluent software has a variety of solutions, providing the multi-grid method to speed up the convergence, meanwhile, parallel computing can work well. So it can provide the optimal and efficient solution to flowing problems on the speed wide range. This article introduces the parallel multi-grid algorithm used in Fluent software, tests and analyzes its parallel performance.

1. MULTI-GRID METHODS IN FLUENT SOFTWARE

The multi-grid method (MGM) is a highly effective serial value computational method. The fine grid relaxation, the coarse grid adjustment and the set of iterative technique are three props of multi-grid method. Its basic idea is using the residual error adjustment characteristic of the coarse grid to eliminate the low frequency component of iteration error, simultaneously using the flaccid smooth characteristic of the fine grid to eliminate the high frequency component of iteration error, the wrapped iterative technique is responsible to solve the same problem through the limit and the interpolation operator to connecting all grid level [1].

The multi-grid method has three basic forms as follows[2]: 1) two-layer V cycle methods, 2) multi-layer V cycle method , 3) full multi-grid method. Fig.1 take the four layers as the example, the graph represents above three methods. In the chart, "○" represents relaxation and iteration; "\" represents restrict; "/" represents interpolation and "□" represents accurate solution.

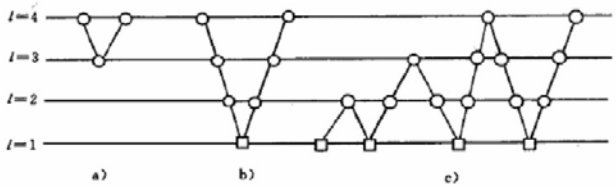


Fig.1. Three Basic Multi-grid Cycles

The multi-grid cycle may be defined as a recursive procedure used in the grid plane when each grid plane passes the grid level, which expands to the next rough grid plane through completing the sole grid cycle in the current plane. The Fluent software has four kinds of multi-grid cycles: V, W, F as well as Flexible cycle. The V and the W cycle can be used in the Algebraic Multi-grid (AMG) and the Full-Approximation Storage (FAS) Multi-grid, the F and the Flexible cycle can only be limitedly used in the AMG method.

Fig.2(a) is V-cycle:

$$\beta_1 smooth \rightarrow restrict \rightarrow Vcycle \rightarrow prolongate \rightarrow \beta_3 smooth$$

Fig.2(b) is W-cycle:

$$\beta_1 smooth \rightarrow restrict \rightarrow Wcycle \rightarrow Wcycle \rightarrow prolongate \rightarrow \beta_3 smooth$$

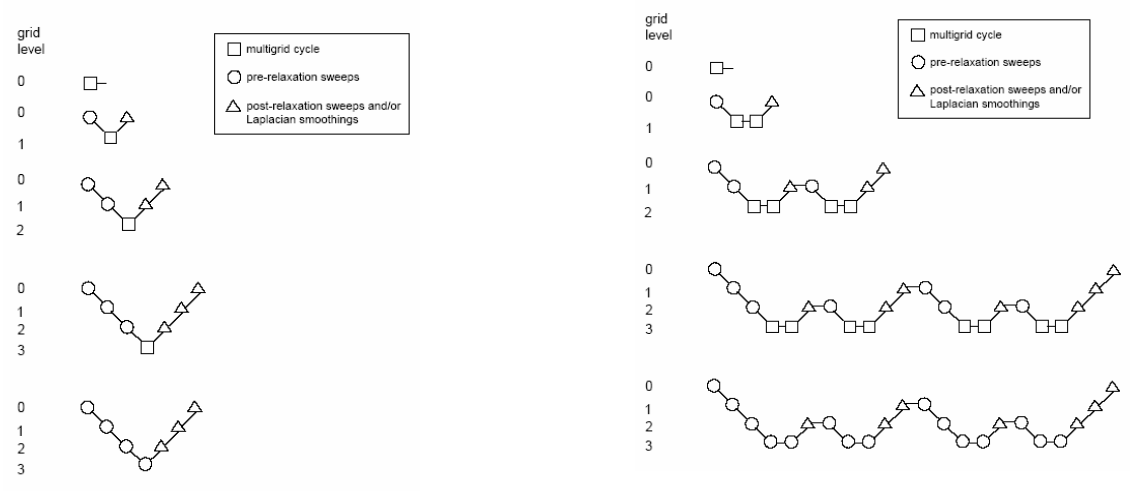
F-cycle:

$$\beta_1 smooth \rightarrow restrict \rightarrow Wcycle \rightarrow Vcycle \rightarrow prolongate \rightarrow \beta_3 smooth$$

As to the V and the W cycle, each plane transformation is controlled by three parameters: β_1、β_2 and β_3. β_1 is used to assign the steps in the current grid plane to carry on the pre-flaccid iteration (in Fig.2 with circular expression),to reduce the high-frequency unit of the local error. In AMG method , The accepted value of β_1 is 0 (i.e.: Not pre-relaxation); β_2 is used to assign the type of the multi-grid cycle, takes 1 and 2 Corresponds the V cycle and the W cycle separately, which can reduce the error of the thick grid (to express with quadrangle in Fig.2); β_3 is used to assign the step of carrying on relaxes iterative (to express With the triangle in Fig.2), which can reduce the high frequency error arising in the multi-grid cycle. in AMG method, The accepted value of β_3 is 1; in FAS method ,the accepted value of β_3 is 0.

The Flexible cycle causes the realization of the coarsening grid computation by the logical control multiple grid procedure, such logical control can guarantee the transference to the rough grid computation when the current plane grid residual error's reducing speed is slow enough .When the current rough grid level's adjustment iterative solution is fully restrained and therefore it should change to the next fine grid, the multi-grid control will deal with it suitably.

*Granted by the Special Scientific Research Foundation for College Doctor Subjects from Ministry of Education of China (No.20050497014).
Corresponding Author: Xiao Jinsheng



（a）V-Cycle （b）W-Cycle

Fig.2. Multi-grid Cycles

The main difference between the Flexible cycle and the V and the W cycle is: The Flexible cycle can determine when and in which frequency to deal with each grid through the satisfactory condition of the common difference of reducing the residual error and the termination criterion; but the V and the W cycle has clearly defined the transforming pattern between each plane.

2. PARALLEL ALGORITHMS IN FLUENT SOFTWARE

Parallel computation in Fluent software uses many computation nodes simultaneously to deal with the same duty. The parallel computation must divide the grid into many subfields, the quantity of subfields is integral times of the number of computation nodes. Each subfield can “dwell” on the different computation node. Besides supporting the parallel computation of single CPU & multi-CPU, Fluent also supports the parallel computation of network distribution. In the Fluent software has been set MPI (Message Passing Interface) parallel mechanism, which largely enhanced parallel performance of parallel computation of the network distribution.

The division form of Fluent software adopts dichotomy principles to carry on, but has no limit to the number of division, and may have the same division number to each processor. The Fluent software provided many kinds of methods to divide the grid, and the most effective division method is related to the problem solved. When grid is divided, the division method to produce grid needs to choose, division number need to be established, the region and the optimized method need to be chosen and so on.

The parallel procedure grid division has three main targets: producing the same quantity unit grid regions; minimizing the division contact field; minimizing neighborhood field of division.

Parallel computing performance can be expressed by the speedup ratio. The general method to calculate the speedup ratio is : In the case of a processor operating a procedure, T_1 as implement time , and P nodes in the parallel machine running the same procedure, if T_P as implement time, then the speedup ratio $S=T_1/T_P$, parallel efficiency $\eta=S/P$ [3].

3. ENVIRONMENTS AND PROCEDURES OF PERFORMANCE TESTS

3.1 Test Environments

Hardware environment: High Performance Computer Cluster (HPCC). The master node is DELL POWEREDGE_2650, matches one Intel Xeon 2.8GHz/533MHz FSB CPU, 2G/DDR266 memory, collection with 2 milliard fold network card, 584G SCSI hard disk; The system includes 8 computation nodes named DELL POWEREDGE_1750, which configures 2 Intel Xeon 2.8GHz / 533MHz FSB CPU, 2G/DDR266 memory, integrated milliard fold network card, 73G SCSI hard disk; Information exchange between the master node and the computation node completes through the milliard fold Ethernet switchboard.

Software environments: Red Hat Enterprise Linux3.0, Fluent6.2.16 for Linux。

3.2 Test Procedures

What the simulation test is the list straight flow channel proton exchange membrane fuel cell. It employs the Fluent software PEM Fuel Cell module to compute and uses Fluent internal command "Benchmark" to alternate 100 steps, and record the CPU utilization ratio and Elapsecl-time. According to the multi grid cycle method, domain decomposition method and the problem solving scale, there are three kinds of plan tests:

Test 1: The grid scale is 1,000,000 units, using the Fluent accepted main axle symmetrical grid broken method and different multi-grid cycle method to test, each computation node assigns a duty.

Test 2: The grid scale is 400,000 units, using the multiple grid cycle method which has the highest Parallel efficiency in Plan 1, and adding 2 computation nodes, each computation node is assigned a duty, adopting different domain decomposition method to carry on the parallel computation. As a result of the fuel cell model geometry characteristic symmetry, this experiment has only adopted Principal X-Coordinate, Principal Y-Coordinate, Principal Z-Coordinate and Cartesian X-Coordinate, Cartesian Y-Coordinate, Cartesian the Z-Coordinate region fission method. In order to facilitate the record, using the short form, such as Principal X-Coordinate’s short form is P X-C.

Test 3: The grid scale has two kinds : the 400,000 units and the 100,000 units, the multiple grid cycle method with highest parallel efficiency is adopted in the plan 1 and the area broken method in plan 2, has 1 to 8 computation nodes, each computation node is assigned a duty.

The master node's participation in the computation can cause the load unbalanced and reduce HPCC's speedup performance[6], therefore in above plans the master node does not participate in the computation, in order to test the accuracy of the result, one test should duplicates three. Because duplication of the test result is extremely good, therefore the experimental result uses the arithmetic mean value of three tests' results.

4. RESULTS AND DISCUSSIONS OF PERFORMANCE TESTS

4.1 Effects of Multi-grid Cycles on Parallel Performance

The one computation node operating time in Test 1 respectively are, V cycle-4786 seconds, W cycle- 37504 seconds, F cycle-5121 seconds, Flexible cycle-6870 seconds. Obviously, the V cycle operating speed is the highest , the W cycle operating speed is the lowest. The analysis thought it is because of the minimum of V cycle operand and the maximum of W cycle operand.

Parallel speedup ratio of various computation nodes of Test 1 are shown in Fig.3. Different methods of computation and communication account for different speedup ratio and computing speed. For the V cycle, the F cycle and the Flexible cycle, computation nodes CPU has high utilization up to more than 90%. So for the three cycles, different test results mainly due to different calculation. But when the W cycle is adopted, the CPU utilization is very low, only up to 10%, and the computing speed is very slow. When the W cycle parallel computation is adopted, communications were considerablely big, which is a major factor.

Fig.3 also shows that the parallel speedup ratios of the four cycle methods are almost the same when computation nodes are less than 5, and the V cycle parallel speedup ratio is significantly greater than the other three when computing nodes continue to increase. With the increase of computing nodes, all growth rates of cycles' speedup ratios gradually become smaller.

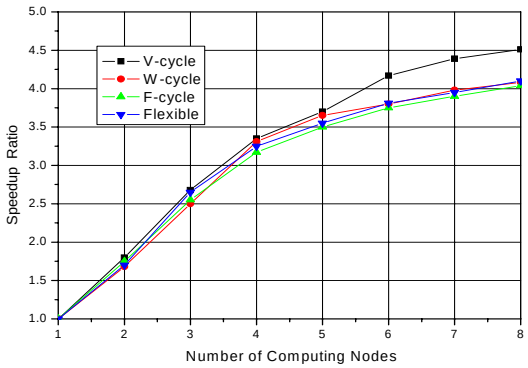


Fig.3. Speedup Ratio of multi-grid cycles

4.2 Effects of Domain Decompositions on Parallel Performance

The test result of Test 2 is shown in table 1. Different domain decomposition computing methods have different time, or even a big difference. Because different domain decomposition generates different interfaces. Different exchange volume of data required by parallel computing causes different communications, and different computing speed. The smaller the Neighborhood fields and segmentation contacts are , the faster the computing speed is. Different models of Solution are suitable for different networks splitting methods, which is in order to compute fastest. In this paper, the best method of splitting the network is Cartesian X-Coordinate.

Table 1 Test results in different domain decompositions

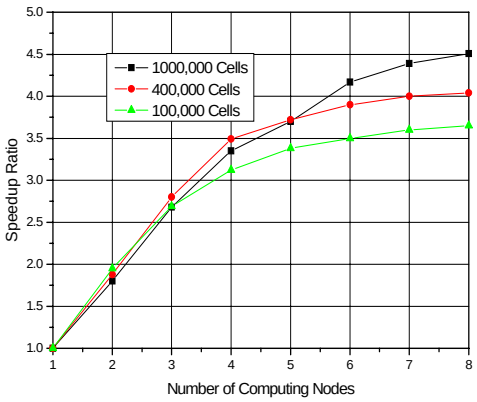
	PX-C	PY-C	PZ-C	CX-C	CY-C	CZ-C
Intercell Ratio(%)	1.0	1.0	0.9	0.2	0.9	0.7
Interface Ratio %	4.8	4.8	5.3	1.0	5.3	4.3
Time (s)	2659	2661	2739	2120	2331	2159

4.3 Effects of Problem Scale on Parallel Performance

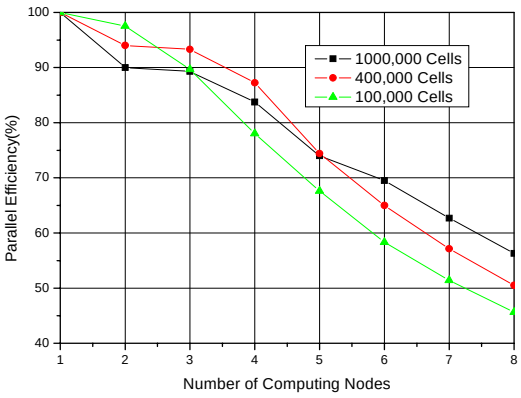
The test result of Test 3 is shown in Fig.4. The same multi-grid cycle method (V cycle) and area splitting method (Cartesian X-Coordinate), and different scale of examples cause different parallel performance. From Fig.4(a) we can see when the computing nodes are few, the different scale of examples basically have same speedup ratio; With a further increase of computing nodes, computing speed and speedup ratio increase, but the growth trend became smaller; the smaller the examples scale are, the smaller the parallel speedup ratio is.

Fig.4 (b) shows that, with the increase of the number of computing nodes, the parallel efficiency reduced; Different sizes of examples have different parallel efficiency. This is because in the message passing model of parallel processing, the amount of computation and communication and relationship between them plays a vital role [4]. With the increase of CPU in computing, CPU utilization and the corresponding computing load on it reduce, but communicating expense on parallel computing increases. Therefore, with the increase of computing nodes, parallel efficiency reduces. For examples of different scale, the relationship between the amount of computation and communication is different and therefore parallel performance is different too.

Fig.5 shows the Comparison of PEM Fuel Cell module speedup ratio, basic modules accelerate ratio[3] in Fluent and ideal highest speedup ratio when they are in the same multi-grid cycle method (V cycle) and grid splitting method (Principal Axes). PEM fuel cell module parallel speedup ratio is smaller than the speedup ratio without that module in Fluent, moreover, both less than ideal speedup ratio, and with the increase of computing nodes the difference increase. The ideal situation has overlooked the influence of the data communications, and PEM Fuel Cell module increase the equation, so computation and communications are greater than the basic module in Fluent.



(A) Speedup ratio



(B) Parallel efficiency

Fig.4. Accelerate performance of different solutions scale

From the comparison of the test results with the Benchmark data[5] provided by FLUENT, we find the parallel efficiency of The test is below Parallel efficiency of DELL POWEREDGE_1750 which the company releases. It shows that further optimization of the test environment is needed.

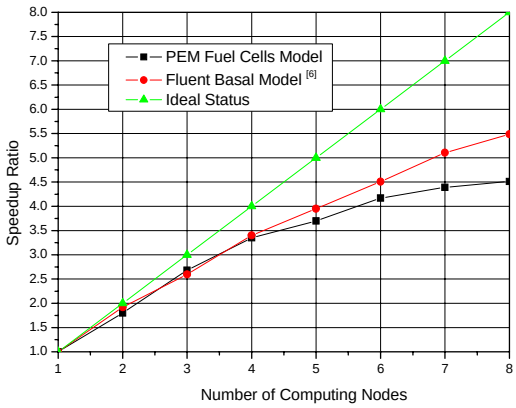


Fig.5. Speedup Ratio

5. CONCLUSIONS

1） The V cycle has the highest computing speed and best parallel performance in the multi-grid cycles of Fluent software.

2） The best way for domain decomposition is trying to produce minimum interfaces between the divided regions, so the shortest time will be needed for communication to solve the problem.

3） Since more unknown variables and communication occur in PEM Fuel Cell module, its parallel performance is not as good as basic modules of Fluent.

4） In order to achieve greater parallel speedup ratio and solving speed, further optimization of the communication between nodes and expansion of DELL HPCC are needed.

REFERENCES

[1] Zhu Zongbo ,Yang Guoxun, Xiao Jinsheng, “Applications of Multi-grid Method in the Numerical Analysis of Heat Transfer,” *[J].Journal of Wuhan Transportation University.* 2000, 24(2):121-124

[2] Zongbo Zhu, Guoxun Yan, Chunxiao Liu, Jinsheng Xiao, “Parallel Multi-grid Algorithm Based on Cluster Computing with Application to Transient Heat Transfer,” *[A].2004 International Symposium on Distributed Computing and Applications to Business, Engineering and Science[C]*, （*DCABES 2004*）,345-349

[3] Wen Xiaofei, Zhu Zongbo, Hu Chunzhi, Xiao Jinsheng, “Performance Evaluation of High Performance Computer Cluster,” *[J].Journal of WUT (Information & Management Engineering)*, 2005, 27(4):19-22

[4] Guo Q P, Yakup P. “Concurrent Communication and Granularity Assessment for a Transputer-based Multiprocessor system,” *[J] Journal of Computer Systems Science & Engineering*, 1990, 5(1): 18-20.

[5] Fluent Inc. Fluent Benchmark[ED/OL], http://www.fluent.com/software/fluent/fl5bench

Adaptive Beamforming Algorithm Based on Inverse QR-RLS for Hexagonal Array Implementation*

Qiang Wang
Safety Engineering Institute, China Jiliang University
Hangzhou, Zhejiang 310018, P.R.China
Email: qiangwang@cjlu.edu.cn ,wangtulip@yahoo.com.cn

ABSTRACT

In shallow water costal areas, to enhance bottomed targets detection performance, a computationally efficient adaptive beamformer based on inverse QR and recursive least-squares (RLS) is developed under Fourier transform framework, for standard hexagonal array implementation. The IQR-RLS algorithm has good numerical stability and can be mapped onto coordinate rotation digital computer processor-based systolic arrays, which is suitable for real time applications. Using the proposed scheme to construct beamformer, which reduces computational complexity significantly and offers better converge rate. The simulation and test results demonstrates the algorithm improves reverberation suppression ability. It improves SNR about 2dB of bottom target detection in reverberation limited area.

Keywords: Active Sonar, Hexagonal Array, Beamforming, Hexagonal FFT, Inverse QR-RLS Algorithm

1. INTRODUCTION

Active sonar involves transmitting an acoustic signal from a source and receiving reflected echoes from the objects of interest, and uses the acoustic signals propagated through the water to detect, classify and localize underwater objects, even to classify marine sediment [1]. Beamformer is the core component of sonar signal processing system. Recently implementing beamforming efficiently becomes an important problem especially in large aperture sonar systems, hexagonal planar array, and 3-D array. The implementation of adaptive beam forming algorithms turns out to be a challenging computational problem due to the high data rate requested and to the ill-conditioning of the interference covariance matrix in typical sonar scenarios. Not surprisingly, the problem motivated the development of systolic algorithms and the investigation of mapping strategies on different parallel computing architectures[2-3].

These sonar array technologies face difficulties, such as low fault tolerance due to computational complexity not readily supported in real-time conventional means that may be overcome with the use of parallel and distributed computing (PDC) technology[4-5]. These challenges in achieving critical levels performance and reliability are particularly difficult to overcome for systems employ high-fidelity beamforming algorithms and must process data from a large number of sensor nodes.

A systolic array for MVDR adaptive beamforming based on inverse QR(IQR) is presented to implement with CORDIC (co-ordinate rotation digital computer) cells [6]. Li proposed a blind beamforming algorithm based on high-order cumulant and neural network, and neural network can operate in parallel structure[7].

Since beamformer is a computation intensive algorithm, some research has concentrated on exploiting constructing fast processing techniques necessary to meet computational requirements of real-world applications[8]. The RLS algorithm offers better convergence rate, steady-state mean square error(MSE), and parameters tracking capability over the adaptive LMS based algorithm. But, RLS filters have been impeded by unstable numerical performance and high computation cost[9], and its performances will seriously degrade due to finite-word-length effects[10]. To circumvent the above difficulties, a numerically robust and computationally efficient procedure to compute the adaptive filter output is known as QR- decomposition. A further advantage of the QR method is that it has a high degree of inherent parallelism which can be exploited to speed up the computation. The triangular systolic array for space-time adaptive processing(STAP) is called IQR and promises an additional decrease of the required computational power[3]. It achieves greater improvement of reducing the computational requirements of the triangular systolic array. Then, RLS based on IQR (IQR-RLS) algorithm is also presented[11], which is the most promising RLS algorithm because it possesses desirable properties for parallel processing.

In this study, a novel hexagonal array(HA) adaptive beamformer using IQR-RLS algorithm implementation under Fourier framewrok is proposed. The algorithm performance is tested by simulated test and lake trial data. It owns high parallelism, suppress the reverberation and meets computation cost requirements of real-time implementation

2. HEXAGONAL ARRAY BEAMFORMER

The motivation of designed HA for the deployment of broad active sonar system is their potential to enhance bottom and buried object detection performance in ocean costal areas. The HA has the best steerable characteristics, and it is the optimal sampling strategy for circularly band limited signals. Hexagonal sampling allows for 13.4% fewer samples than rectangular sampling. Moreover, HA owns vertical spatial resolution[1][11].

2.1 HA Conventional Beamformer

The conventional beamformer(CBF) under Fourier transform framework supplies a quickly, efficient method for real-time implement in practice. In Fig.1, we show a finite area sequence corresponding to one of hexagonally periodic sequence. Discrete fourier transform of hexagonal sampling signal (HDFT) and hexagonal fast Fourier transform(HFFT) were firstly proposed in reference[11]. The discrete hexagonal Fourier transform is shown as Eq. (1):

$$X(k_1,k_2)=\sum_{n_1}\sum_{n_2}x(n_1,n_2)\,\mathrm{e}^{\left[-j\frac{\pi}{3N}(2n_1-n_2)(2k_1-k_2)+\frac{\pi}{N}(n_2k_2)\right]} \qquad (1)$$

* the project supported by China Jiliang University(XZ0513) and partially National Natural Science Foundation of China (No. 50676088)

where $u_x=cos\theta$, $u_y=cos\Phi$, θ is incident signal elevation angle, Φ is incident signal azimuth angle, λ is wave length.

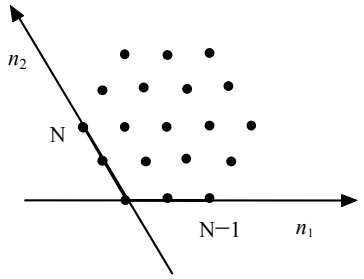


Fig. 1. Schematic hexagonal sampling of hexagonal array

$$k_1=\frac{3d}{2\lambda}Nu_x+\frac{\sqrt{3}d}{2\lambda}Nu_y, k_2=\frac{\sqrt{3}d}{\lambda}Nu_y$$

The CBF of regular HA is written as:

$$y=\sum_{n_1}\sum_{n_2}x(n_1,n_2)\exp\{j2\pi\frac{d}{\lambda}[\frac{\sqrt{3}}{2}n_2u_y+(n_1-\frac{n_2}{2})u_x]\} \quad (2)$$

To wide-band signal, we modify the narrow band model and use correct terms to guarantee the beam with different frequency f and wavenumber k point the same bearing angle.

$$S_{1m}=k_1\cdot(f_m-f_p)/f_p, S_{2m}=k_2\cdot(f_m-f_p)/f_p$$

where p means reference frequency. To a random frequency f_m, (k_1,k_2) directs the same spatial cosine $u_{x,p}$, $u_{y,p}$. The Eq. (1) is written as:

$$X(k_1,k_2)=\frac{1}{3N^2}HDFT(x(n_1,n_2))**$$
$$HDFT(\exp\{-j[\frac{\pi}{3N}(2n_1-n_2)(2S_{1m}-S_{2m})+\frac{\pi}{N}n_2S_{2m}]\}) \quad (3)$$

where ** denotes hexagonal two-dimension convolution. So there exists a fast algorithm HFFT to improve computation efficiency. The array beamforming response **v** can be expressed in vector form as:

$$\mathbf{v}(n_1,n_2)=\exp\{j2\pi\frac{d}{\lambda}[\frac{\sqrt{3}}{2}n_2u_y+(n_1-\frac{n_2}{2})u_x]\} \quad (4)$$

From Fig.1., the HA element coordinates in non- orthogonal axes is (n_1,n_2). The $\mathbf{v}(n_1,n_2)$ has the similar structure with HDFT.

3. ADAPTIVE BEAMFORMING OF HA

3.1 MVDR Beamformer

The objective of beamforming is to resolve the direction of arrival of spatially separated signals within the same frequency band. The sources of the signals are located far from the sensor array. Therefore, the propagating wave is a plane wave and the direction of propagation is approximately equal at each sensor. We also neglect the effect of multipath propagation caused by reflection. The sensor outputs are multiplied by the weights and summed to produce the beamformer output. The beamformer output is a spatially filtered signal with an improved SNR over that acquired from a single sensor: minimum variance distortionless response (MVDR)[1].

The signal model as receiving array data include: desired signal $s(n)$, interference $i(n)$ and $\mathbf{w}(n)$ white Gaussian noise. It is presented as:

$$\mathbf{x}(n)=\mathbf{s}(n)+\mathbf{x}_{i+n}(n)=\mathbf{v}(\mathbf{k}_s)s(n)+\sum\mathbf{v}(\mathbf{k}_i)i(n)+\mathbf{w}(n) \quad (5)$$

MVDR stems from minimizing the array's overall output power (i.e. variance) whilst preserving the target signal impinging from the desired look direction.as measured in the direction of the wanted signal, may be described simply as a measure of signal-to-noise-plus- interference ratio (SNIR).

$$\mathrm{SINR}_{out}=\frac{\left|\mathbf{c}^H\mathbf{s}(n)\right|^2}{E[\left|\mathbf{c}^H\mathbf{x}_{i+n}(n)\right|^2]}=\frac{\sigma_s^2\left|\mathbf{c}^H\mathbf{v}(k_s)\right|^2}{\mathbf{c}^H\mathbf{R}_{i+n}\mathbf{c}}$$

where σ_s^2 is signal power, $\mathbf{R}_{i+n}$ is covariance matrix of interference plus noise.

3.2 Sequential MVDR Algorithm and Performance

The adaptive beamforming with MVDR is divided into three tasks. The first task is the averaging of the CSDM. The second task is matrix inversion, which inverts the exponential average of the CSDM. The third task is steering, which steers the array and calculates the power for each steering direction[5].

The averaging task consists of n^2 complex multiplications and additions followed by n^2 divisions, to compute the estimate of the CSDM, which results in a computational complexity of $O(n^2)$. The number of operations required in estimating the CSDM could be reduced by making use of the Hermitian property of the CSDM. However, the computational complexity of this task would still remain at $O(n^2)$[14]. The inversion algorithm we use for the matrix inversion task is IQR-RLS. The steering task is responsible for steering the array and _nding the output power for each of the steering directions. The main operation in the steering task is the product of a row vector by a matrix then by a column vector, which results in $O(n^2)$ operations. This operation must be performed once for every steering direction, which increases the execution time linearly as the number of steering directions increases.

3.3 HA MVDR Beamformer

The MVDR beamforming outputs of HA is:

$$y(n)=\mathbf{c}_o^H\mathbf{x}(n)=\frac{\mathbf{v}^H(u_x,u_y)}{\mathbf{v}^H(u_x,u_y)\mathbf{R}_{i+n}^{-1}\mathbf{v}(u_x,u_y)}\mathbf{R}_{i+n}^{-1}\mathbf{x}(n) \quad (6)$$

Covariance matrix $\mathbf{R}_{i+n}$ is positive define Hermite matrix, Cholesky decomposition is used to gain Eq. (7):

$$\mathbf{P}_{i+n}=\mathbf{R}_{i+n}^{-1}=[\tilde{\mathbf{R}}_{i+n}^H\tilde{\mathbf{R}}_{i+n}]^{-1}=\tilde{\mathbf{R}}_{i+n}^{-1}\tilde{\mathbf{R}}_{i+n}^{-H} \quad (7)$$

Then weight vector $\boldsymbol{C}$ of HA MVDR is written as :

$$\mathbf{c}_o=\frac{\tilde{\mathbf{R}}_{i+n}^{-1}\tilde{\mathbf{R}}_{i+n}^{-H}\mathbf{v}(u_x,u_y)}{\mathbf{v}^H(u_x,u_y)\tilde{\mathbf{R}}_{i+n}^{-1}\tilde{\mathbf{R}}_{i+n}^{-H}\mathbf{v}(u_x,u_y)}=\frac{\tilde{\mathbf{R}}_{i+n}^{-1}\tilde{\mathbf{R}}_{i+n}^{-H}\mathbf{v}(u_x,u_y)}{\left|\mathbf{v}^H(u_x,u_y)\tilde{\mathbf{R}}_{i+n}^{-1}\right|^2} \quad (8)$$

Based on Eq.(6)，the hexagonal FFT MVDR is concluded,

$$y(n)=\frac{\mathbf{v}^H(u_x,u_y)\tilde{\mathbf{R}}_{i+n}^{-1}\tilde{\mathbf{R}}_{i+n}^{-H}\mathbf{x}(n)}{\mathbf{v}^H(u_x,u_y)\tilde{\mathbf{R}}_{i+n}^{-1}\tilde{\mathbf{R}}_{i+n}^{-H}\mathbf{v}(u_x,u_y)}=\frac{\mathbf{v}^H(u_x,u_y)\mathbf{Z}(n)}{\left|\mathbf{v}^H(u_x,u_y)\tilde{\mathbf{R}}_{i+n}^{-1}\right|^2} \quad (9)$$

3.4 Adaptive Beamforming Based on IQR-RLS

To RLS adaptive beamformer, its weight vector **c** is written as

$$\mathbf{c}_{rls}(n)=\frac{\tilde{\mathbf{R}}^{-1}(n)\tilde{\mathbf{R}}^{-H}(n)\mathbf{v}(n)}{\mathbf{v}^H(n)\tilde{\mathbf{R}}^{-1}(n)\tilde{\mathbf{R}}^{-H}(n)\mathbf{v}(n)} \quad (10)$$

Iterating weight vector **c** to update $\tilde{R}^{-1}(n)$ or R(n) with numerical stability is the key point. Conventional RLS algorithm becomes numerically unstable when R(n) losses its Hermitian symmetry. We need not calculate inversion of matrix $\tilde{R}^{-1}(n)$. There exists a unit orthogonal matrix $\mathbf{Q}(K)$ meets Eq. (11) requirement.

$$\mathbf{Q}(n)\begin{bmatrix} \frac{1}{\sqrt{\lambda}}\tilde{\mathbf{R}}^{-H}(n-1)\mathbf{x}(n) & \frac{1}{\sqrt{\lambda}}\tilde{\mathbf{R}}^{-H}(n-1) \\ 1 & \mathbf{0}^{\mathrm{H}} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \tilde{\mathbf{R}}^{-H}(n) \\ \frac{1}{\sqrt{\alpha(\mathrm{n})}} & \frac{\mathbf{g}^{H}(n)}{\sqrt{\alpha(\mathrm{n})}} \end{bmatrix} \quad (11)$$

The Eq. (11) shows, to update $\tilde{R}^{-H}(n)$ from $\tilde{R}^{-H}(n-1)$, we need to search unit orthogonal matrix $\mathbf{Q}(n)$ and make elements of $\tilde{\mathbf{R}}^{-H}(n-1)\mathbf{x}(n)/\sqrt{\lambda}$ are zero. The IQR-RLS initial value is $\tilde{\mathbf{R}}^{-H}(-1)=\delta^{-1}\mathbf{I}$. The IQR-RLS is used to implement optimum beamforming.

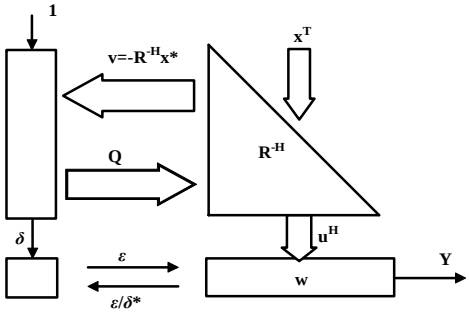


Fig. 2. RLS-IQR array structure

The RLS-IQR array is schematically represented in Fig. 2. where ε is least squares residual. The triangular array computes the matrix-vector $\mathbf{v}=-\mathbf{R}^{H}\mathbf{x}^{*}$ from right to left and passes the resulting vector $\mathbf{v}$ to the left-hand column[3], [6]. The latter generates the rotation parameter and feed back to to the triangular array to update $-\mathbf{R}^{H}$. Similarly, the bottom row calculates the predicted residual $\varepsilon=\mathbf{y}-\mathbf{x}^{T}\mathbf{w}$, and pass it to the processor in the lower-left corner, which generates the parameter ε/δ^{*} and feeds it back to the bottom row for weight update, according to Eq. (12).

$$\mathbf{w}(n)=\mathbf{w}(n-1)-\varepsilon(n)\bullet\mathbf{u}(n)/\delta^{*}(n) \quad (12)$$

Note that therc are two computational steps taking place on the RLS-IQR array: matrix-vector multiplication, which proceeds from right to left, and triangular update, which proceeds in the opposite direction. The IQR array still offers pipelined weight extraction using roughly half the number of processors but with more complicated interconnections owing the presence of contraflow[3].

A novel fast algorithm: combined HFFT-RLS with IQR-RLS is proposed in this study. Because using IQRD-RLS algorithm directly update $R^{-1}(n)$' s Cholesky decomposition $\tilde{R}^{-1}(n)$. Therefore, output of HFFT IQR-RLS adaptive beamforming is

$$y(n)=\frac{HDFT(\tilde{\mathbf{Z}}(n))}{\left|HDFT(\tilde{\mathbf{R}}^{-1}(n))\right|^{2}} \quad (13)$$

where $\tilde{\mathbf{Z}}(n)=\mathbf{R}^{-1}(n)\mathbf{x}(n)$. Using IQR-RLS algorithm to update covariance matrix $R^{-1}(n)$, the $R^{-1}(n)$ satisfy positive definite Hermite characteristic. This method owns good numerical stability and high computation efficiency, compared with HFFT CBF.

3.5 Complexity of HFFT IQR-RLS Algorithm

Most of the computations in beamforming consist of vector and matrix operations with complex numbers. The number of complex multiplication of beamforming involved has main effect on computation speed. To narrow-band signal, a regular HA at horizonal direction has maximum element N_x, the total elements of array is $N=1+3(N_x^2-1)/4$, each side of hexagon owns elements is $N_1=(N_x+1)/2$.

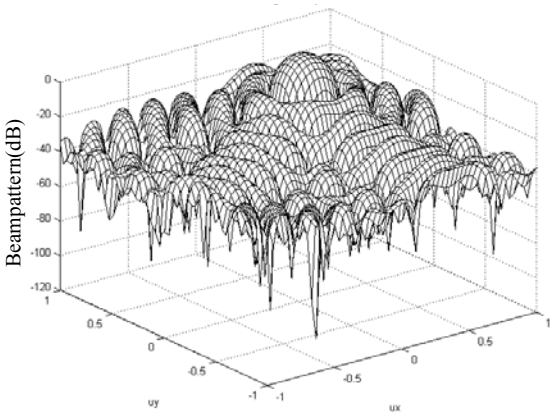
To form $3N^2$ beams, CBF needs real number multiply operations $3N^2*3N^2=9N^4$, this is a most intensive stage with $O(N^4)$ complexity, while HFFT beamforming algorithm just needs $N^2/\log_2 N$ operations. The number of multiplication operations required to generate the beamforming output increase rapidly.

If RLS beamforming to form $3N_x^2$ beams, it will require $N^3 + N^2 + 3N_1^2(N^2+2N)$ complex multiplications. While, HFFT IQR-RLS just needs $N^3 + N^2 + 3N_1^2 + (9N_1^2\log_2 N_1 + 8N_1^2)(N+1)$ complex multiplications. To 91-element HA(N_x=11), number of complex multiplications is reduced about 60%.

4. SIMULATION TEST

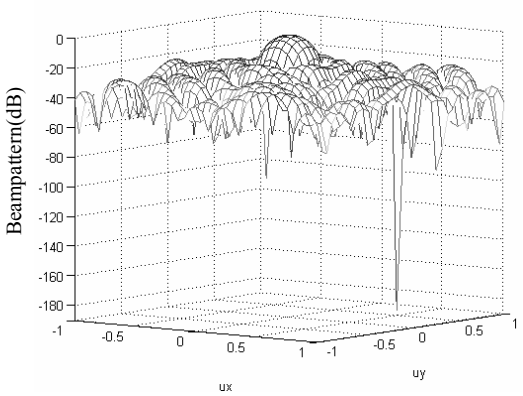
To evaluate the proposed method of nulling-steering and interference suppression capability of beamforming algorithms. In simulation, a standard HA with 91 elements (interelement =0.1m), input signal is sine signal, cosine of DOA is u_x=0, u_y=0, and SNR=20dB. The received signal in each hydrophone consists of a desired signal in the presence of a interference from incident angle u_x=0.5, u_y=0.5 and white Gaussian noise. interference and noise ratio(SINR) is 60dB. Consider a narrowband array with N isotropic receiving sensor elements.

After 1000 times iteration, the beampatterns of HFFT CBF and MVDR is shown in Fig.3 (a-b). From the simulation test, it turns out MVDR beampattern keep the high main beam and low side–lobe spatial response. It has the good null-steering capability. But HFFT CBF beampattern exists high grating lobe, mean weight vector $\mathbf{w}$ doesnot converge and loses numerical stability.



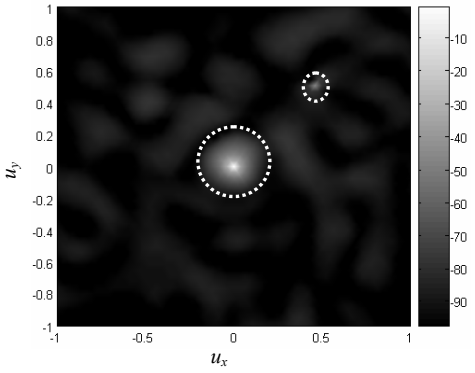
(a) HFFT CBF beampattern

To examine the capability of interference suppression, the results in terms of nulling capability, are shown in Fig. 4. The HFFT IQR-RLS algorithm outperforms the HFFT CBF. The simulation condition is the same as the Fig. 3. The SNR= 20dB, and a stochastic interference incident angle (u_x=0.46, u_y=0.51), SINR=60dB. HFFT IQR-RLS BF can identify the target signal and disturbance(in the dashed circle), while HFFT CBF is not able to differentiate target and disturbance signals, target source is covered by strong interference.

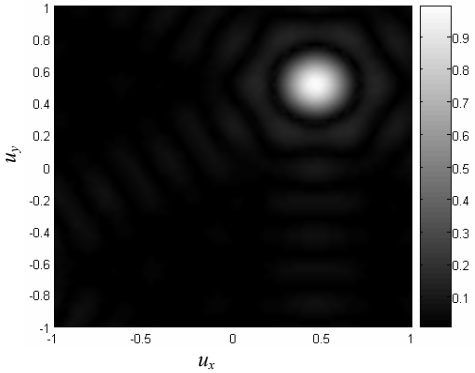


(b) Hexagonal array MVDR beamformer

Fig. 3. HFFT CBF and MVDR of HA



(a) 91-element HA HFFT IQR-RLS BF results



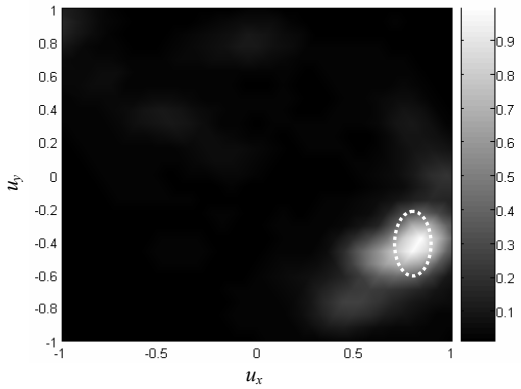
(b) 91-element HA HFFT BF results

Fig. 4. Comparison of HFFT-IQR-RLS and HFFT CBF

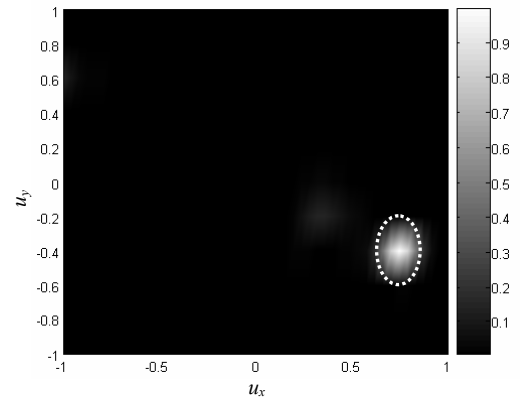
5. ANALYSIS WITH REAL DATA

During a recent lake trial, data were gathered for off-line beamforming analysis. The equipment used consisted of a receiving hexagonal array(91 hydrophones) within the circular area (radius is 0.5m). Bottomed target conducted in reverberation-limited condition. Transmitted LFM signal: band width 5-10kHz, pulse delay is 5ms and sampling frequency is 50kHz.

The outputs is normalized cumulative energy, and axis of abscissa is u_x (after sampling conversion), vertical coordinate is u_y. The true target location(θ,Φ) is (67°, 333°). The Target is marked in the dashed ellipse area. The Fig. 5(a) presents HFFT CBF results and Fig.2(b) presents HFFT IQR-RLS beamforming results. From Fig. (b), the target signal is seriously interfered by bottom reverberation. The target location is not obvious, while in Fig. (a), the target location area's energy is enhanced, the corresponding location exists bright speck. The bright spot outside of the circle area caused by the reverberation in the main beam bin of beamformer, because test is conducted in reverberation-limited area. The Fig. 5(a-b) shows output presentation for the bottom target echo HFFT IQR-RLS. The bright spot out of the dashed epplise is caused by the reverberation in the beamformer main beam.



(b) Outputs of HFFT CBF



(b) Output of HFFT-IQR-RLS beamforming result

Fig. 5. HFFT-IQR-RLS results comparison with HFFT CBF

On the whole, MVDR beamforming based on IQR-RLS gains high space resolution to improve the target localization accuracy and effectively suppress strong reverberation. The SNR is improved about 2dB of the proposed adaptive beamforming algorithm, compared with CBF.

6. CONCLUSIONS

An adaptive beamforming algorithm based IQR-RLS under Fourier framework for hexagonal array is presented. In the iteration decomposition, the sequential workload is divided into the number of processor stages and these stages are overlapped in execution by pipelining. Including its simulated and lake test results. The authors concluded:

(1) Expressed adaptive beamforming of HA under Fourier framework, and their computational efficiency improved and easy to perform in parallel algorithm.

(2) Beamforming IQR-RLS algorithm under HFFT which reduces computational complexity significantly as well as guarantees numerical stability to implementation in practice.

(3) It enhances detection performance in reverberation-limited area, The SNR of beamforming outputs improves about 2dB. By taking advantage of the proposed algorithm

parallelism for in-array sonar processing, the techniques can be applied to more advanced beamforming algorithms such as match-field processing.

REFERENCES

[1] S. Stergiopoulos(Ed.), *Advanced Signal Processing Handbook: Theory and Implementation for Radar, Sonar, and Medical Imaging Real Time Systems*, Boca Raton: CRC Press, 2000.

[2] A. George, J. Markwell, R. Fogarty, "Real-time sonar beamforming on high-performance distributed computers", *Parallel Computing*, Vol. 26, No.10, 2000, pp. 1231~1252.

[3] A. Farina, L.Timmoneri, "Real-time STAP techniques", *IEE Colloquium on Space-Time Adaptive Processing* Apr 1998, pp. 3/1-3/7

[4] P. Sinha, A. George, K. KIM, "Parallel Algorithms for Robust MVDR Beamforming", *Journal of Computational Acoustics*, Vol. 10, No. 1, 2002 , pp.69~96

[5] A. George, J. Garcia, K. Kim, P. Sinha, "Distributed Parallel Processing Techniques for Adaptive Sonar Beamforming", *Journal of Computational Acoustics*, Vol. 10, No.1, 2002, pp. 1~23.

[6] P. Bollini, et al, "QR Versus IQR algorithms for adaptive signal processing: performance evaluation for radar applications", *IEE Proc Radar, Sonar Navigation*., Vol. 143, No. 5, Oct. 1996, pp.328~340.

[7] Li Hongsheng, Zhao Junwei, "Study of A Blind Beamforming Method Suitable for Hardware Realization in Underwater Acoustic Environment", *ACTA ACUSTICA*, July, 2003, Vol. 28, No.4, pp. 339~344.

[8] Van Trees, H. L, *Optimum Array Processing*, New York: John Wiley & Sons, Inc., 2002.

[9] Chern, S. J., Chang. C.Y., "Adaptive Linearly Constrained Inverse QRD-RLS beamforming algorithm for moving jammers suppression", *IEEE Trans*. *On Antennas and Propagation*, Vol.50, No.8, Aug 2002, pp.1138~1150.

[10] J.G.Proakis et al, *Algorithms for Statistical Signal Processing*, New York: Person Education, Inc., 2002.

[11] S.T. Alexander, A.L. Ghirnikar, "A method for recursive least squares filtering based upon an inverse QR decomposition", *IEEE Trans. Signal Processing*, Vol.41, No.1, Jan 1993, pp.20~30.

[12] R. M. Mersereau, "The Processing of Hexagonally Sampled Two-dimensional Signals", IEEE Proc, Vol.67, No. July 1979, pp. 930~949.

[13] J. Lam, A. C. Singer, "Fast Adaptive Bayesian Beamforming using the FFT", *Proceedings of the IEEE Workshop on Statistical Signal Processing*, St Louis, MO, Sep 2003, pp. 413~416

[14] Ehrhardt, J. C., "Hexagonal Fast Fourier Transform with Rectangular Output", *IEEE Trans. Signal Processing,* Vol.41, No.3, Mar 1993, pp. 1469~1472.

[15] J.G. McWhirter, T.J. Shepherd, "Systolic Array Processor for MVDR beamforming", *IEE Proceedings,* Vol. 136, Pt. F, No. 2, April 1989, pp. 75~80.

Qiang Wang is an associate Professor in College of Metrological Technology & Engineering, China Jiliang University. He graduated from Zhejiang University in 2005; Ph.D major in control theory and engineering. Post doctoral in electronic engineering of Zhejiang University from 2005 to 2007. He is currently a Senior Research Associate with intelligent sensor system, in China Jiliang University. He has published over 10 Journal papers. His research interests are in parallel sonar signal processing, optic fiber sensor

Multi-objective Optimization Using Genetic Simulated Annealing Algorithm*

Wanneng Shu
College of Computer Science, South-Central University for Nationalities
Wuhan, 430074, China
Email: shuwanneng@yahoo.com.cn

ABSTRACT

In many real-life problems, objectives under consideration conflict with each other, and optimizing a particular solution with respect to a single objective can result in unacceptable results with respect to the other objectives. A reasonable solution to a multi-objective problem is to investigate a set of solutions, each of which satisfies the objectives at an acceptable level without being dominated by any other solution. In this paper, an overview and tutorial is presented describing genetic simulated annealing algorithm (GSAA) developed specifically for problems with 0/1 knapsack problem. Experimental results have shown that GSAA is superior to genetic algorithm (GA) and simulated annealing (SA) on performance.

Keywords: Multi-objective Optimization, Genetic Simulated Annealing Algorithm, Genetic Algorithm, Simulated Annealing

1. INTRODUCTION

The objective of this paper is present an overview and tutorial of multiple-objective optimization methods using GSAA. For multiple-objective problems, the objectives are generally conflicting, preventing simultaneous optimization of each objective. Many, or even most, real engineering problems actually do have multiple-objectives, i.e., minimize cost, maximize performance, maximize reliability, etc. These are difficult but realistic problems [1]. GSAA is an optimal algorithm combing GA with SA that is particularly well-suited for this class of problems. GSAA are customized to accommodate multi-objective problems by using specialized fitness functions and simulated annealing to promote solution diversity.

In this paper a GSAA for solving complex multi-objective optimization problems precisely and efficiently is presented based on GA and SA. The experimental results show the superiority of the QGSAA in terms of optimization quality, efficiency. The organization of the remaining content is as follows; in section 2 is the definition of multi-objective optimization problem, in section 3 GSAA is proposed, in section 4 is the feasibility analysis of GSAA, in section 5 simulations on 0-1 knapsack problem is carried out to investigate the effectiveness of the GSAA. Finally we end with some conclusions in section 6.

2. THE DEFINITION OF MULTI-OBJECTIVE OPTIMIZATION PROBLEM

In the multi-objective optimization scenario there are m incommensurable and often conflicting objectives that need to be optimized simultaneously. We formally define the MOP as follow [2]:

Definition 1(Multi-objective Optimization Problem (MOP)). An m-objective optimization problem includes a set of n decision variables $X = (x_1, x_2, \ldots, x_n)$, a set of m objective functions $F = (f_1, f_2, \ldots, f_m)$, and a set of k constraints $C = (c_1, c_2, \ldots, c_k)$ .The objectives and the constraints are functions of the decision variables. The goal is to:

Maximize/Minimize: $F(X) = \{f_1(X), f_2(X), \ldots, f_m(X)\}$,

Subject to the constraints: $C(X) = \{c_1(X), c_2(X), \ldots, c_m(X)\} \le (0, \ldots, 0)$.

The collection of decision variables (X) constitute the decision space. The set of objective values (F) form the objective (solution) space. In some problem definitions, the constraints are treated as objective functions, the objectives may also be treated as constraints to reduce the dimensionality of the objective-space.

3. THE GENETIC SIMULATED ANNEALING ALGORITHM

Genetic algorithm (GA) is efficient heuristic search methods based on Darwinian evolution with powerful characteristics of robustness and flexibility to capture global solutions of complex optimization problems [3]. Although GA has a powerful quality of global search, it is liable to raise the problem of prematurely convergence in the practical application, and has low search efficiency in the late evolving period [4, 5]. SA originations from the method of the statistical physics and first employed by Kirkpatric to solve the optimization problem, on the other hand, has a more powerful local search ability, but it depends more on parameter. GA is weak in local search but powerful in global search while SA is weak in global search but powerful in local search. Thus, GSAA can greatly enhance the running efficiency of algorithm and its solution quality by fully combining the advantages of GA and SA.

The Solution Process of GSAA as follows:

(1) Generate the initial annealing temperature T_0 , the population scale M , t =0;
(2) Encode and generate initial population $P(t)$ randomly;
(3) Conduct the operations as follows at the current temperature T_t ;
(4) Estimate the fitness value of each individual in population $P(t)$;
(5) Make a reproduction process of $P(t)$ to generate the father population $F(t)$.
(6) Make a crossover process of $F(t)$ to generate the

*This paper is supported by National Natural Science Foundation of China (Grant No. 60473085)

crossover population $C(t)$;

(7) Make a mutation process of $C(t)$ to generate the medium population $M(t)$;

(8) Generate the new population $P(t+1)=F(t) \bigcup M(t)$. By combining the father population $F(t)$ with the medium population $M(t)$;

(9) When the terminal condition is coincident, the annealing process will natural end; otherwise, t=t+1, $T_{t+1} = T_t \times (1 - \frac{t}{M})$, go back to (3);

4. THE FEASIBILITY ANALYSIS OF GSAA

The following theorems can be achieved by proving the literature [6] and [7]:

Theorem1: the well necessary condition for the convergence of GAGA (Global Annealing Genetic Algorithm) is to allow the father population to participate in the competition

Theorem2: if the annealing temperature T_n of GAGA meets $\sum_{n=1}^{\infty} e^{-\delta/T_n} < +\infty$, well the $\exists n_0$, when $n \geq n_0$, $\overline{f(p_n)}$ is plus limitary below saddle sequence and converge to global optimal solution, namely $p\{\lim_{n\to+\infty} \overline{f(p_n)} = f^*\} = 1$, $p\{\lim_{n\to+\infty} [p_n \in M]\} = 1$. M is the global optimal solution. $\overline{f(p_n)}$ is the average fitness value of the population P_n. f^* is the maximum fitness value of the population. $\delta = \min\{|f(x) - f(y)|; f(x) \neq f(y)\}$ is the minimum subtract value of different fitness value.

Lemma 1: GSAA can converge to the global optimal solution

Proof. In the process of solution, GSAA combines the father population F_k and the medium M_k into the next population P_{K+1}, namely $P_{k+1}=F_k \bigcup C_k$, which is a typical GAGA algorithm. Hence GSAA can converge to the global optimal solution.

5. EXPERIMENT AND RESULTS ANALYSIS

The knapsack problem, a kind of combinatorial optimization problem, is used to investigate the performance of GSAA. The knapsack problem can be described as selecting from various items those items which are most profitable, given that the knapsack has limited capacity. The 0-1 knapsack problem is described as that given a set of m items and a knapsack; select a subset of the items so as to maximize the profit $f(x)$:

$$f(x) = \sum_{i=1}^{m} p_i x_i$$

$$\sum_{i=1}^{m} w_i x_i \leq C \quad , \quad x_i \in \{0,1\}, 1 \leq i \leq m$$

Where $x = [x_1 \quad x_2 \quad \ldots \quad x_m]$, p_i is the profit of item i, w_i is the weight of item i, and C is the capacity of the knapsack.

For the purpose of comparison, we test the GA, SA and GSAA on the knapsack problems with 300,500 items, respectively. the population size consider for GA, SA and GSAA is equal to 100.the initial annealing temperature T_0=1.

To better evaluate the quality of the algorithm, E_m is set as the relative error which is used to measure the optimal degree of the algorithms to the problem, and the idea is that the smaller the value is, the better optimal quality the algorithm has; E_f as the fluctuation rate which is used to measure the approach degree of the algorithm with the random initial value and the idea is that the smaller the value is, the higher reliability is.

$$E_m = \frac{C_1 - C^*}{C^*} \times 100\% \qquad E_f = \frac{C_2 - C^*}{C^*} \times 100\%$$

In the formula, C_1 is the actual optimal value attained in the running process of the algorithm; C^* is the anticipant optimal value of problem. C_2 is average value attained by multi-operation of the algorithms[8].

Tab.1-2 shows the experimental results of the knapsack problem found by GA, SA and GSAA within 500 generations over 10 runs for 300 and 500 items. The major parameters employed in the algorithm such as the population scale M =100, the initial annealing temperature T_0 =1, the terminal annealing temperature is 0, the crossover and mutation probability are 0.85 and 0.05 respectively. The comparisons of best profits and average profits of population are shown in Fig.1-4.The result show that GSAA performs well in spite of small size of population, which yields superior results as compared to GA and GSAA.

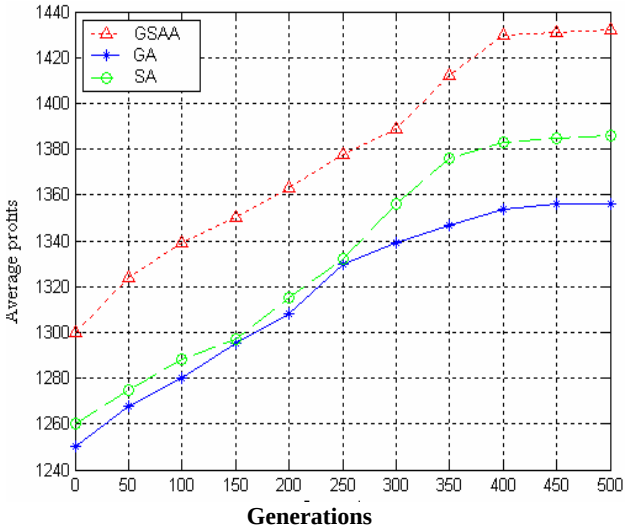


Fig.1. The comparison of average profits (300 items).

Table 1. Experimental results of the knapsack problem on Profits

Number of items	Profits	GA	SA	GSAA
300	best	1476.7	1510.2	1523.1
	mean	1356.5	1385.1	1432.3
	worst	1132.1	1268.2	1270.5
500	best	2720.1	2973.7	3041.8
	mean	2534.6	2802.9	2885.7
	worst	2190.4	2346.3	2386.2

Table 2. Experimental results of the knapsack problem on Profits on E_m and E_f

Number of items	Relative error E_m (%)			Fluctuation rate E_f (%)		
	GA	SA	GSAA	GA	SA	GSAA
300	0.23	0.21	0.13	0.12	0.11	0.06
500	0.18	0.17	0.10	0.15	0.15	0.04

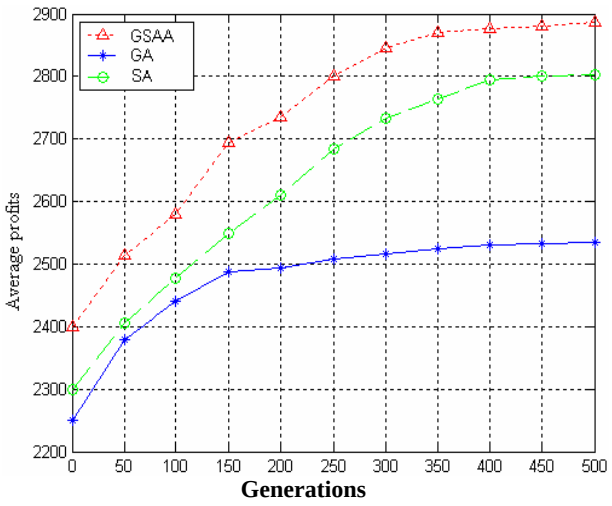


Fig.2. The comparison of average profits (500 items)

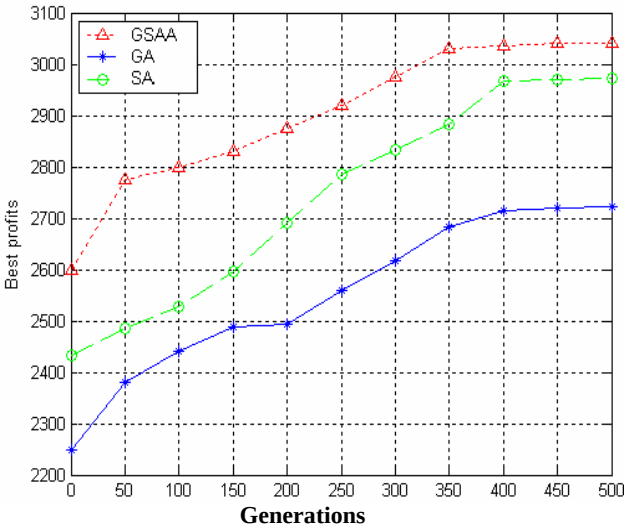


Fig.4. The comparison of best profits (500 items)

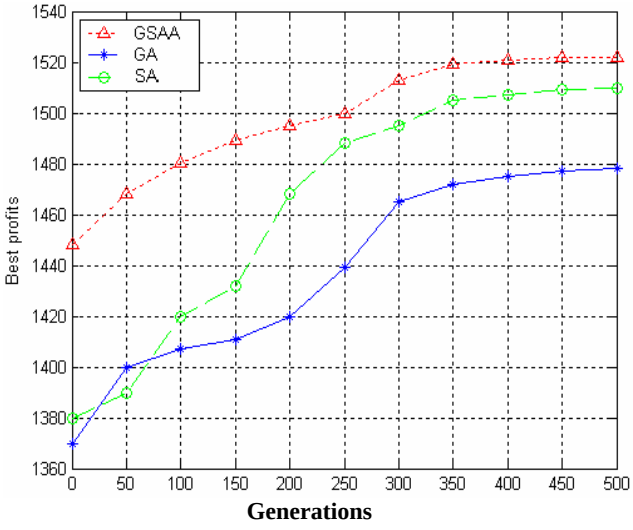


Fig.3. The comparison of best profits (300 items)

6. CONCLUSIONS

Most real-world engineering problems involve simultaneously optimizing multi-objectives where considerations of trade-offs is important. In the last decade, evolutionary approaches have been the primary tools to solve real-world multi-objective problems. This paper presented GSAA that have great advantages over traditional methods for solving multi-objective optimization problems, since they can be applied simultaneously with integer, discontinuous or discrete design variables; the experimental results of the knapsack problem demonstrate the effectiveness and the applicability of GSAA. Further theoretical analysis of GSAA will be investigated and equation of annealing temperature will also be investigated.

REFERENCES

[1] P.A.N.Bosnan,D.Thierens, "The balance between proximity and diversity in multi-objective evolutionary algorithm," *IEEE Trans.* Evolutionary Comput.7 (203) 174-188.

[2] K.Deb,A.Pratap,S.Agarwal,T.Meyarivan. "A fast and elitist multi-objective genetic algorithm: NSGA-II," *IEEE Trans.* Evolutionary Comput.6 (2002)182-197.

[3] Z.Michalewicz, *Genetic Algorithms + Data Structure=Evolution Programs,* 3rd., Berlin, Springer-Verlag, 1996, Cha.4.

[4] K.H.Han,J.H.Moore,"Genetic quantum algorithm and its application to combinatiorial optimization problem[A]." *Proceedings of the 2000 IEEE Congress on Evolutionary Computation*[C],USA:IEEE Press,2000.

[5] L.C.Jiao,L.Wang, "A novel genetic algorithm based on immunity," *IEEE Trans.*on System,Man and Cybernatic, 30(2000)5,552-561.

[6] ZHANG Jiang-She, XU Zong-Ben, LIANG Yi."Global Annealing Genetic Algorithm and its convergence well necessary condition [J]." *SCIENCE IN CHINA(Series E)* , 1997，27（2）：154~164.

[7] WANG Xia, ZHOU Guo-Biao. "Strong Convergence (a.s.) of Global Annealing Genetic Algorithm." *MATHEMATICA APPLICATA*，2003，16 (3):1~7.

[8] Wanneng Shu, Shijue Zheng, Li Gao, Shangping Dai and Jianhua Du, "An Improved Genetic Simulated Annealing Algorithm Applied to Task Scheduling in Grid Computing," *Proceedings of The First International Conference on Complex Systems and Applications*,June 16-18, 2006, Huhhot, China, Watam Press.

A Parallel QPSO Algorithm Based on Neighborhood Topology Model

Peng Wang, Jun Sun, Wenbo Xu
School of Information Technology, Southern Yangtze University
Wuxi, Jiangsu 214122, China
Email: wpengyu@163.com

ABSTRACT

Quantum-behaved Particle Swarm Optimization algorithm (QPSO) is a new population-based search strategy, which has good performance on well-known numerical test problems. QPSO is based on the standard Particle Swarm Optimization algorithm and the theory of quantum physics. In this paper, we realize the parallel QPSO based on the Neighborhood Topology Model, which is much closer to the nature world. The performance of the paralleled QPSO is compared to PSO and QPSO on a set of benchmark functions. The results show that the parallel QPSO outperforms the other two algorithms.

Keywords: Quantum-behaved PSO, Neighborhood Topology Model, Parallel Computing.

1. INTRODUCTION

Recently, more and more large-scale engineering optimization problems impose large computing demands, resulting in the large requirement of High Performance Computers. But it can't satisfy all requirements even if we have expensive hardware. Then Parallel Computing becomes an effective method for solving the large-scale computational problems and paralleled GA and SA algorithms have been successfully applied to solve Combinatorial Optimization problems [1]. Particle Swarm Optimization (PSO) algorithm is a novel population based evolutionary algorithm, which is originally introduced by Kennedy and Eberhart in 1995 [2]. PSO has fewer parameters than either GA or SA algorithms. It also has shown to be comparable in performance with GA and SA. In [3], Sun et al. introduced quantum theory into PSO algorithm. The experiment results indicate that the QPSO algorithm works better than standard PSO on several benchmark functions.

In the paper, we present a parallel QPSO algorithm based on a revised Neighborhood Topology Model and a novel constriction parameter of QPSO is proposed. The proposed algorithm has shown its superior performance on several benchmark functions than PSO and QPSO.

The paper is organized as follows: In section 2, we introduce the Standard PSO and QPSO algorithms. In Section 3, we explain the proposed Neighborhood Topology Model and its application in the new parallel QPSO algorithm. Experimental results are described in Section 4. A conclusion is in Section 5.

2. PSO AND QPSO ALGORITHM

In PSO, the position of particle i at (t+1)th iteration is updated by the following formula:

$$v_i(t+1) = w * v_i(t) + C_1 * rand(\cdot) * (p_i - x_i(t)) + C_2 * Rand(\cdot) * (p_g - x_i(t)) \quad (1)$$

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (2)$$

Where C_1 and C_2 are positive constants, and rand (-) and Rand (-) are two random functions in the interval [0, 1]. X_i represents the ith particle, V_i represents the rate of the position change for particle i. P_i represents the best previous position of particle, P_g represents the best particles in the population. Variable w is the inertia weight [4].

In [5], Sun introduced a global point called Mainstream Thought or Mean Best Position of the population into PSO that represents the creativity of particle. The algorithm is called QPSO and the update formula of particle's position is defined as follows:

$$mbest = \frac{1}{M}\left(\sum_{i=1}^{M} P_i\right) = \left(\frac{1}{M}\sum_{i=1}^{M} P_{i1}, \ldots, P_{id}\right) \quad (3)$$

$$x_{id} = P_{id} \pm \beta * |mbest_d - x_{id}| * ln\left(1/u\right) \quad (4)$$

$$P_{id} = \varphi * P_{id} + (1-\varphi) * P_{gd}, \varphi = rand() \quad (5)$$

where $mbest$ is the Mean Best Position of the population, P_{id}, a stochastic point between P_{id} and P_{gd}, is the local attractor on the dth dimension of the ith particle, φ is a random umber distributed uniformly on [0,1], parameter M is the population size and P_i is its own best position seen so far of particle i, which is usually named as $PBest$. β is called Creativity Coefficient and u is a random number uniformly distributed in (0, 1). The QPSO algorithm is described as follows.

Initialize the population
Do
  find out $mbest$ using equation (3)
  for i =1 to population size M
    if $f(x_i) < P_g = min(P_i)$ then $P_i = X_i$
    $P_g = min(P_i)$
    for d=1 to dimension DIM
      $fi_1 = rand(0,1)$
      $fi_2 = rand(0,1)$
      $P = (fi_1 * P_{id} + fi_2 * P_{gd}) / (fi_1 + fi_2)$ (6)
      $u = rand(0,2)$
      if $rand(0,1) > 0.5$ $X_{id} = P - L * ln(1/u)$ (7)
      else $X_{id} = P + L * ln(1/u)$ (8)
Until termination criterion is met.

3. PARALLEL QUANTUM-BEHAVED PSO ALGORITHM BASED ON NEIGHBORHOOD TOPOLOGY MODEL

The QPSO has the characters of lying on less parameter, easy to be implemented and global search ability. But like many other evolutionary algorithms, the QPSO algorithm tends to suffer from premature convergence in strongly multi-model test problems, which results in great performance loss and

sub-optimal solutions. This is due to a decrease of diversity in search space, diversity declines rapidly, leaving the QPSO algorithm with great difficulties of escaping local minima. Another problem in QPSO is computational cost. With the dimension of the problem increasing, the population size must be enlarged to ensure a good performance, which will greatly increase the computationally expensive.

To solve the problems mentioned above, we propose a novel operator *LBest* (i.e. local best solution) to replace the variable *GBest* (global best position) and introduce the parallel mechanism based on Variable Neighborhood Topology Model into QPSO algorithm. Although several modifications to the original Quantum-behaved particle swarm algorithm have been made to improve and adapt it to specific types of problems, a parallel version of QPSO based on the fine-grained model has not been previously implemented.

3.1 The variable neighborhood topology model

In the PSO algorithm, each particle records the coordinates and the best fitness value associate with the best solution that particle achieved so far, which is called *PBest* . The PSO algorithm also maintains the coordinates and the value of the best solution achieved by the whole population, which is called *GBest* . In our implementation, we use the best solution within a neighborhood that is called *LBest* solution and it can be discovered by inspecting all *PBest* solutions within the neighborhood.

The Neighborhood Topology Model (NTM) presented in this paper is a gradually variable neighborhood operator [7]. The advantage of the NTM is that the subpopulations can search diverse regions of the problem space. During the initial stages of search procedure, the particle's neighborhood is itself. As the search procedure going on, the neighborhood is extended to all the particles, in other words, from *LBest* to *GBest* .

The proposed algorithm employs the Variable Neighborhood Topology Model and the whole population is partitioned into *N* subpopulations, where *N* is the number of PUs (Processor Units). One PU has only one part of particle swarm (the ideally size of subpopulation is 1). All the PUs communicate periodically and exchange the *LBest* . The communication is a synchronous voting that the *LBest* of a subpopulation is broadcast to all the PUs. In this paper, we employ a ring structure of NTM that one PU is allotted 10 particles, the neighborhoods of particle i are defined as P_{i-n} , … P_{i-1} , P_i and P_{i+1} … P_{i+n} ; At the same time, the processor PU_i 's neighborhoods are defined as P_{i-1} , PU_i and PU_{i+1} . Each particle stores the *LBest* position received from other counterparts in its local memory and each processor stores the *GBest* position of its own subpopulation, and then selects a best one randomly at each iteration to adjust their position according to the equation (4).

At the beginning of the search, processor 0 initials and allots all the particles. Each processor receives the allotted particles and then evolves independently. At the early stage, the population diversity is high. As exploration is more important than exploitation at this stage, the PUs should work on the local subpopulation independently for a longer period of time. The PUs communicate each other and exchange their *LBest* periodically which follows an exponentially decreasing sequence: initially |*MIter*/2|, then |*MIter*/4|, and so on, where *MIter* is the maximum number of iterations. As some individuals in one subpopulation influenced another to focus on one local optimum, another part of the population could search around another. The flow of information from one part to another is moderated by the necessity of "persuading" intermediate individuals to search in a particular area. Once better positions are found in that region, they can influence their neighbors and all the particles at the end. At the beginning, the parallel QPSO algorithm based on VNTM prevent from Premature Convergence by maintaining "multi-centre of gravitation". At the later stage, the population converges to a number of different *LBest* . Thus, exploitation of more promising position is needed to avoid unnecessary work on optimizing the local *GBest* positions.

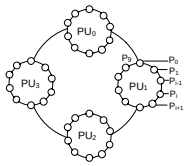


Fig.1. *LBest* Neighborhood

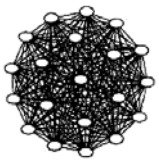


Fig.2. *GBest* Global Model Topology Model [9]

We call the proposed Parallel QPSO Algorithm as parallel NT-QPSO and the procedure is outlined as below:

3.2 Parallel QPSO algorithm based on the VNTM

Step1: Initialize population which include *M* particles with random x_i ;

Step2: Partition the whole population into *N* subpopulations with *size* equal to *M*/*n*, and then broadcasts them to the different CPU;

Step3: for each of the subpopulation, Para do

1) Evaluate desired optimization fitness function of local population;
2) Find the *mbest* and *LBest* of local population;
3) Change the position of the particle according to the equations (6) (7) (8);

Step4: Exchange the *LBest* with neighborhood particles and replace it's num if *LBest* better;

Step5: if (*t* is reached N or *LBest* extend to *GBest*)

Gather all *LBest* ;

Random choose *LBest* of local subpopulation;

Step6: exit

4. EXPERIMENTS AND RESULTS

To test the performance of parallel NT-QPSO algorithm, three benchmark functions are used. The experiments are implemented by VC++6.0 and MPI. The number of PC for constituting the cluster environment is 2, 4 and 8. Three functions are Rastrigrin Function, Shaffer Function and Griewank Function. These functions are all minimization problems with minimum value zero. Table 1 lists the initialization ranges and the maximum position values (*Xmax*) for all the functions. The fitness value is set as function value.

We had 40 trial runs for every experiment. The results of the averaged fitness value for 40 runs are in table 2 to table 5. Different population sizes *M* are used for each function with different dimensions. The population sizes are 40 and 80. The maximum iteration is set to 1000, 1500 and 2000 corresponding to the dimensions 10, 20 and 30.

Table 1. Benchmark functions and parameter

Functions	Benchmark functions	Initialization Range	Search Domain
Rastrigrin	$\sum_{i=1}^{n}(x_i^2 - 100\cos(2\pi x_i) + 10)$	(2.56,5.12)	10
Griewank	$\frac{1}{4000}\sum_{i=1}^{n}(x_i-100)^2 - \prod_{i=1}^{n}\cos(\frac{(x_i-100)}{\sqrt{i}}) + 1$	(300,600)	600
Shaffers	$0.5 + \frac{(\sin\sqrt{x^2-y^2})^2 - 0.5}{(1.0+0.001(x^2+y^2))!}$	(30,100)	100

Table 2. Results of Rastrigrin function

M	DIM	Gmax	SPSO	QPSO	Parallel NT-QPSO		
					2CPU	4CPU	8CPU
40	10	1000	3.5978	3.5685	3.3469	2.4073	2.3984
	20	1500	16.4337	11.2532	10.3829	8.9475	7.7643
	30	2000	37.2796	23.1281	18.4926	16.7216	15.9981
80	10	1000	2.6047	2.1445	0.72165	0.57403	0.41028
	20	1500	13.5826	10.2798	4.02859	2.67977	1.9943
	30	2000	29.2193	16.7769	10.5321	8.2298	6.37712

Table 3. Results of Griewank function

M	DIM	Gmax	SPSO	QPSO	Parallel NT-QPSO		
					2CPU	4CPU	8CPU
40	10	1000	0.08524	0.06912	0.06011	0.04517	0.03702
	20	1500	0.02719	0.01698	0.01499	0.01083	0.01012
	30	2000	0.01573	0.01161	0.00961	0.00742	0.00535
80	10	1000	0.07562	0.03719	0.03097	0.02279	0.00205
	20	1500	0.02958	0.0175	0.0150	0.0120	0.0097
	30	2000	0.01258	0.01126	0.01011	0.0054	0.0043

Table 4. Results of Shaffer function

M	DIM	Gmax	SPSO	QPSO	Parallel NT-QPSO		
					2CPU	4CPU	8CPU
40	2	2000	0.0012	0.0018	0.0012	0.00085	0.00063
80	2	2000	0.0002	0.0004	0.0003	0.00012	0.00002

From the results, we can see that parallel NT-QPSO outperforms SPSO and QPSO when population size is larger than 20. If the population size is less than 20, the result of parallel NT-QPSO may be worse than SPSO. The reason is that the particles can't form a community as there's less particle for a processor. As the averaged cost time is concerned, parallel NT-QPSO is the least among the three algorithms.

5. CONCLUSIONS

In this paper, a new parallel QPSO based on Variable Neighborhood Topology Model algorithm is proposed. The proposed model has the advantages that subpopulations can search diverse regions of the problem space and global convergence is guaranteed. The search ability has been improved and has fewer chances to trap into the local minima. The experiment results show that the proposed algorithm outperforms the standard PSO and QPSO on benchmark functions, proving its efficiency.

REFERENCES

[1] Pooja P. Mutalik *et al*, "Solving Combinatorial Optimization Problems Using Parallel Simulated Annealing and Parallel Genetic Algorithms", *ACM 1992*, pp. 1031-1038.

[2] J. Kennedy and R. C. Eberhart, "Particle Swarm Optimization", Proc. *IEEE Conference on Neural Network*, 1995, pp. 1942-1948.

[3] Sun Jun and Xu Wenbo, "Particle Swarm Optimization with Particles Having Quantum Behavior", *Proc. 2004 IEEE Congress on Evolutionary Computation*, pp. 325-331.

[4] Y. Shi, R. C. Eberhart, "A Modified Particle Swarm," Proc. 1998 *IEEE International Conference on Evolutionary Computation*, pp. 1945-1950.

[5] Sun, Jun, et al, "A Global Search Strategy of Quantum-behaved Particle Swarm Optimization". *Proc. of IEEE Conference on Cybernetics and Intelligent Systems*, 2004, pp.111~116.

[6] G. Venter and BC. Watson, "Exploiting parallelism in general purpose optimization", *Proc. 6th International Conference on Applications of High-Performance Computers in Engineering*, Maui, Hawaii, 2000

[7] James Kennedy and Rui Mendes, "Population Structure and Particle Swarm Performance", *IEEE*, 2002

[8] J. F. Schutte et al, "Parallel Global Optimization with the Particle Swarm Algorithm", John Wiley & Sons, 2003

[9] James Kennedy, "The particle swarm: Social adoptions of knowledge", *IEEE*, 1997

Peng Wang, male, master graduate student, his research involves in Parallel Computing, Computing Intelligence, AI;

Wenbo Xu, male, Full Professor, his research interests are in the artificial intelligence, the computer control, inserts the type operating system, the parallel computation, the pattern recognition;

Sun Jun, male, doctor graduate student, his research interests are in financial computation, evolution computation.

The Sufficient Conditions of A Graph with Two H-cycles Having No Common Edges

Fugui Liu
Science college, Wuhan University of Technology
Wuhan, China 430063
Email: lufugui620@163.com

ABSTRACT

Let G be a simple graph of n order and randomly take $e_1, e_2 \in E(G), G-\{e_1,e_2\}$ is 2—connected. graph If $f<n, \delta \geq 5, f-\delta \geq \frac{n}{2}+2$, then G includes two H-cycles that have no common edges. This paper gives a simple proof of the theorem $(\delta \geq 6)$, and points out that the theorem also holds when $\delta = 4$, unless G belongs to a special kind of graph.

Keywords: Graph, Connected Graph, Hamilton Cycle

1. INTRODUCTION

The graph we discuss is a simple undirected graph in this paper. Let G be a graph, denote $E_G(A,B)=\{uv \in E(G) \mid u \in A \subset V(G), v \in B \subset V(G)\}$, $e_G(A,B)=|E_G(A,B)|$, Other symbols and terms could be seen in literature [1]. Especially, we use *H*—cycle to note Hamilton cycle; use *H*—graph to note Hamilton graph; use G_0 to note those graphs which have the following features: $V(G)=X \cup Y$, while $x=\{x_0,x_1,x_2,x_3,x_4\}$, $Y=V(G)-X$, and $G[X]$ is K_5 or $K_5-x_3x_4$ $\forall y \in Y$, $d_G(y) \geq f-4 \geq \frac{n}{2}+2$, $3 \leq e_G(x_i,Y) \leq u-5$ $(i=3,4), u=|V(G)|$.

Zhu Yongjin and Li Hao briefly proved the following theorem 1 in literature [1].

Theorem1 Let G be a simple graph of n order and randomly take $e_1, e_2 \in E(G)$, $G-\{e_1,e_2\}$ is 2 — connected graph. If $f<n, \delta \geq 5$, $f-\delta \geq \frac{n}{2}+2$, then G includes two H—cycles with no common edges. Two issues has been pointed out in this article by Zhu Yongjin and Li Hao: (1) How to simply prove theorem 1? (2) Is theorem 1 tenable for $\delta = 4$?

This paper aims to answer the above two questions.

2. THE SIMPLE PROOF OF THEOREM 1

First of all, introducing some lemmas:

Lemma 1[3] G has H—cycle if and only if $\overline{G}$ has H —cycle.

Lemma 2[1] suppose *u, v* are the disconnected vertex, which belong to the graph G of n order, note $T_G(u,v)=V(G)-[N_G(u) \cup N_G(v) \cup \{u,v\}]$, $T_{G'}(u,v)=\{\omega \in T_G(u,v) \mid d_G(\omega) \geq |T_G(u,v)| + \max\{2, n-d_G(u)-d_G(v)\}\}$, If $d_G(u)+d_G(v)+|T_{G'}(u,v)| \geq n$, then G is H — graph if and only if $G+uv$ is H — graph.

Lemm3 Let G satisfy the conditions of theorem 1, $x_1, x_2 \in V(G)$ and $d(x_i) \leq \delta + 2 (i=1,2)$, then $x_1x_2 \in E(G)$.

Proof suppose $x_1x_2 \notin E(G)$, then $d(x_1)+d(x_2) \geq f \geq \frac{n}{2}+\delta+2$, and $n > f > \frac{n}{2}+\delta+2$, yields $\frac{n}{2} > \delta+2$, so $d(x_1)+d(x_2) > 2\delta+4$, which contradicts $d(x_i) \leq \delta + 2 (i=1,2)$, therefore, $x_1x_2 \in E(G)$. Note $X=\{v \in V(G) \mid d_G(v)=\delta\}$, $Y=\{v \in V(G) \mid d_G(v) \geq f-\delta\}$, and $Z=\{v \in V(G) \mid \delta < d_G(v) < f-\delta\}$.

The simple proof of theorem1$(\delta \geq 6)$:

Obviously, $\forall x \in X$, $z \in Z$, $y \in Y$ has $xz \in E(G)$, $d_G(y) \geq f-\delta \geq \frac{n}{2}+2$, $|Z \cup X| \leq \delta+1$, $|Y| \geq n-\delta-1$. Using the inversion method, suppose that G is not such a graph with the greatest number of edges in the graphs, which satisfies the above given conditions, then it could be proved : $\forall u,v \in V(G)$, $uv \notin E(G)$ has $d(u)+d(v) \leq n+3$ (otherwise suppose a H—cycle of G is C, let $G_1=G-C$, basing on the assumption, G_1 has the H —path $u \cdots v$, since $d_{\overline{G_1}}(u)+d_{\overline{G_1}}(v) \geq d_G(u)-2+d_G(v)-2 \geq n$, so $uv \in E(\overline{G_1})$, thus, G_1 has H —cycles, which is a contradiction. As a result, $G[Y]$ is clique. Taking C from H —cycle of G, let $G_1=G-E(C)$, and letting G_1 have the greatest connected degree. Firstly, to prove G_1 is 2—connected. Otherwise, suppose $k(G_1) \leq 1$, let $\overline{Y}_1=Y \cup \{v \notin Y, e_{G_1}(v,Y) \geq 2\}$, $\overline{Y}_i=\overline{Y}_{i-1} \cup \{v \notin \overline{Y}_{i-1}, e_{G_1}(v,\overline{Y}_{i-1}) \geq 2\}, i \geq 2$, $\overline{Y}=\bigcup_{i=1}^{\infty}\overline{Y}_i$, $\overline{X}=V(G)-\overline{Y}$. Obviously, $G_1[\overline{Y}]$ is 2 —connected. The following will prove that $G[\overline{X}]$ is clique.

If there is $x_1, x_2 \in \overline{X}$, $x_1x_2 \notin E(G)$, then $d_G(x_i) \leq |\overline{X}|+1$ $(i=1,2)$, basing on lemma3, suppose $d_G(x_2) \geq \delta+3$, then $\delta+3 \leq d_G(x_2) \leq |\overline{X}|+1$, so $|\overline{X}| \geq \delta+2$, which, obviously, contradicts $|\overline{X}| = |X \cup Z| \leq \delta+1$. As a result, $\overline{X}$ is a clique in G.

Furthermore, because G_1 is not 2 — connected, only two situations will occur as following:

(1) G_1 is unconnected. $G_1[\overline{X}]$ *and* $G_1[\overline{Y}]$ are two subgraphs. In this case, $|\overline{X}| \geq 5$ (because of $\delta \geq 6$), so that $\overline{Y} \cap X = \Phi$.

When $\overline{Y} \cap Z = \Phi$, since bot $G[\overline{X}]$ and $G[\overline{Y}]$ are clique, and $|\overline{X}| \geq 5$, take H—cycle C of G, so that $|E_G(\overline{X},\overline{Y}) \cap E(C)| = 2$, basing on the conditions, $G_1 = G - E(C)$ is 2—connected. This is a contradiction.

When $\overline{Y} \cap Z \neq \Phi$, suppose $|\overline{X}| = k$, Obviously, $5 \leq k \leq \delta + 1$, $|\overline{Y}| = n - k$, $\forall x \in \overline{X}$ has $d_G(x) \leq k + 1$. Since $k \geq 5$, for $z \in Z \cap \overline{Y}$, there must exist $x \in \overline{X}$ so that $xz \overline{\in} E(G)$ Therefore, $d_G(z) \geq f - d_G(x) \geq f - k - 1 \geq \frac{n}{2} + \delta - k + 1 > \frac{1}{2}(|Y| + 3)$. Thus, $G_1[\overline{Y}]$ is H— connected, and then take C from H---cycle G, so that $|E_G(\overline{X},\overline{Y}) \cap E(C)| = 2$, basing on the conditions, $G_1 = G - E(C)$ is 2—connected, which is a contradiction.

(2) Connected G_1 has cut –edge e or cut-vertex v_0. Now delete the cut-dege e or cut-vertex v_0, thus, it could be proved just like (1). Therefore, G_1 is 2 — connected graph. Randomly take $x_0 \in X$, $y \in Y$, and check $T_{G_1}(x_0, y)$. Obviously, $t_{\overline{G_1}}(x_0, y) = |T_{\overline{G_1}}(x_0, y)| \leq 2$.

Since $\forall u \in T_{\overline{G_1}}(x_0, y)$, as $\delta \geq 6$, so that $d_{\overline{G_1}}(u) \geq \delta - 2 \geq 4 \geq t_{\overline{G_1}}(x_0, y) + 2$.

According to lemma2, we could know $x_0 y \in E(\overline{G_1})$, so $\overline{G_1}[Y \cup X]$ is clique, therefore, for $\forall y \in Y$, $d_{\overline{G_1}}(y) \geq n - \delta - 1$; for $\forall x \in X$, $d_{\overline{G_1}}(x) \geq n - 2 - 1$, Thus, $d_{\overline{G_1}}(x) = n - 1$. Note $Z_1 = \{z \in Z \mid d_G(z) \geq \delta + 3\}$, According to Lemma3, we know $G[Z - Z_1]$ is clique. For $\forall z \in Z_1, y \in Y$, we have $d_{\overline{G_1}}(z) + d_{\overline{G_1}}(y) \geq \delta + 1 + n - \delta - 1 = n$. Therefore, $yz \in E(\overline{G_1})$, as a result, $\overline{G_1}[Y \cup Z_1 \cup X]$ is clique. $\forall u \in Z - Z_1$, $v \in Y \cup Z_1 \cup X$, since $G[Z - Z_1]$ is clique, so that $t_{\overline{G_1}}(u, v) = |T_{\overline{G_1}}(u, v)| \leq 2$, and $\forall w \in T_{\overline{G_1}}(u, v)$, thus, we have $d_{\overline{G_1}}(w) \geq \delta - 2 \geq 4 \geq t_{\overline{G_1}}(u, v) + 2$. According to lemma2, we know $uv \in E(\overline{G_1})$, so $\overline{G_1}$ is a complete graph. Basing on lemma1, we can get that G_1 has H —cycles, which is a contradiction. As a result, G has two H—cycles without common edges.

3. THE SITUATION OF δ=4

Theorem 2. Suppose G is a simple graph of n order, and $\forall e_1, e_2 \in E(G), G - \{e_1, e_2\}$ is 2—connected graph. If $f < n$, $\delta = 4$, $f > \frac{n}{2} + 6$, then G includes two H—cycles without common edges, unless G belongs to G_0.

Proof Take $x_0 \in V(G), d_G(x_0) = 4, N_G(x_0) = \{x_1, x_2, x_3, x_4\}$, $Y = V(G) - N_G(x_0) - \{x_0\}$, Obviously $|Y| = n - 5$, $\forall y \in Y$, we have $d_G(y) \geq f - 4 \geq \frac{n}{2} + 2$, Similar to the above simple proof, we suppose $G[Y]$ is clique. According to the condition, $N_G(x_0)$ has at most 3 nodes whose degree are 4.

(1) $d_G(x_1) = 4, d_G(x_i) \geq 5 \quad (i = 2,3,4)$

If $\forall x \in \{x_2, x_3, x_4\}$, we have $x_1 x \in E(G)$, since $d(x_i) \geq 5$ $(i = 3,4,5)$, and according to connected conditions, there at least exist $y_2, y_4 \in Y$, so that $x_2 y_2, x_4 y_4 \in E(G)$, make the H—cycle of G, $H_1 : y_2 x_2 x_0 x_3 x_1 x_4 y_4 \cdots y_2$. According to 2—connected features, there exist $y_3', y_4' \in Y$, so that $x_3 y_3', x_4 y_4' \in E(G_1)$, and $G_1 = G - E(H_1)$ (Suppose). When $x_2 x_3 \in E(G)$, obviously, we can get H — cycle of G_1, $H_2 : x_0 x_1 x_2 x_3 y_3' \cdots y_4' x_4 x_0$;when $x_2 x_3 \overline{\in} E(G)$, since $f \geq 13$, there exists at least ore node whose degree (in G) is not less that 7 in x_2, x_3. If $e_{G_1}(x_3, Y) \geq 1$, $e_{G_1}(x_3, Y) \geq 4$, then, it is easy to make the H—cycle of G_1.

If there at least exist $x_1 x_4 \overline{\in} E(G)$, $G[Y \cup \{x_4\}]$ is clique. Now make the H—cycle of G, $H_1 : y_2 x_2 x_0 x_3 x_1 y_1 \cdots y_2$. Similarly, it is not hard to prove based on the connected conditions.

(2) $d_G(x_i) \geq 5 \quad (i = 1,2,3,4)$

If there exists x_1, such that $x_0 x_1 \in E(G)$, similar to (1) it is not hard to prove. So suppose $N_G(x_0)$ is independent preset among G, since $f \geq 13$, suppose $d(x_i) \geq 7$ （$i = 2,3,4$）, $d(x_1) \geq 5$, randomly take H — cycle H_1 of G, let $G_1 = G - E(H_1)$, then there at least exist 4 nodes in Y, $d_{\overline{G_1}}(y) \geq 2n - 5$, so $y x_i E(\overline{G_1}) \quad (i = 2,3,4)$, then $d_{\overline{G_1}}(y) \geq 2n - 3$. Furthermore, $x_1 y \in E(\overline{G_1})$, $x_0 y \in E(\overline{G_1})$, it is not hard to make H—cycle of G_1.

(3) $d_G(x_i) = 4$, $d_G(x_i) \geq 5 \quad (i = 1,2,3)$

Now $N_G(x_0) - \{x_4\}$ is clique in G. From the connected conditions, for $\forall x \in \{x_1, x_2, x_3\}$, we have $x x_4 \overline{\in} E(G)$, then $G[Y \cup \{x_4\}]$ is clique. According to the conditions, there must exist $y_i \in Y$, so that $x_i y_i \in E(G)$（$i = 1,2,3$）. The two Hamilton cycles that have no common edges of G are $x_1 x_0 x_1 x_2 x_3 y_3 \cdots x_4 and y_1 x_1 x_3 x_0 x_2 y_2 \cdots y_1$.

(4) $d_G(x_1) = d_G(x_2) = 4, d_G(x_i) \geq 5$ （$i = 3,4$）

If $\forall x \in \{x_1, x_2\}$, $x' \in \{x_3, x_4\}$, we have $x x' \in E(G)$. Now G belongs to G_0. Obviously, there is no two H—cycles that have no common edges. If there at least exists $x_1 x_4 \overline{\in} E(G)$, then $Y \cup \{x_4\}$ is clique in G, when $d_G(x_3) \geq f - 4 \geq \frac{n}{2} + 2$, $G[Y \cup \{x_3, x_4\}]$ is clique. Now because $x_1 x_4 \overline{\in} E(G)$, there exists $y_1 \in Y$, so that $x_1 y_1 \in E(G)$. It is not hard to make two H—cycles that have no common edges.

When $d_G(x_3) < f - 4$, $N_G(x_0) - \{x_4\}$ is clique in G. Then

$y_1 \in Y$, as a result, $x_1 y_1 \in E(G)$; if $\forall x \in \{x_2, x_3\}, \forall x' \in \{y_1, x_4\}$, we have $xx' \in E(G)$, then we can make two *H*—cycles: $y_1 x_1 x_3 x_0 x_2 x_4 \cdots y_1, x_4 x_0 x_1 x_2 x_3 y_1 \cdots x_4$. It is not hard to make two *H*—cycles without common edges in other situations.

4. CONCLUSIONS

Hamilton Cycle was named for problems of traveling the world proposed by Hamilton in 1856. At present, we have achieved several necessary and sufficient conditions about Hamilton graphs while we have not got "if and only if" conditions about it. It is a hot topic in this field. The two problems proposed in literature [1] have been answered in this paper, which plays a fundamental role for studying Hamilton problems, and has the potential for computer applications.

REFERENCES

[1] Yongjin Zhu, Hao Li, "The progress of Hamilton problem in Graph Theory," *Journals of Qufu Education University*, Vol.2, 1985, pp.70-74.

[2] Yongjin Zhu, Hao Li, "The research of Hamilton problems in Graph Theory," *Journals of Qufu Education University*, Vol.4, 1983, pp.36-40.

[3] J. A. Bondy, and U. S. R. Murty, *Graph Theory with Applications*, London, Macmillan, 1976.

Parallel Recommender Algorithm Based on Immune Theory

Yidan Su [1], Yucai Wang [2]
[1] Business School, University of Shanghai for Science and Technology
Shanghai 200093, China Country
[2] College of Computer and Electronics Information, Guangxi University
Nanning,Guangxi , 530004, China
Email: [1] Ydsu2002@163.com, [2] allenair@126.com

ABSTRACT

The immune system has a lot of features, such as diversity, distribution and self-organizing. In this work, we present two new improved algorithms based on Steve's study. Our algorithms can improve the real-time response speed of Steve-algorithm largely. Finally, we also show experiments in which the proposed method provides a better recommendation performance on MovieLens data set.

Keywords: Immune System, Collaborative Filtering, Recommender Algorithm, Response Speed

1. INTRODUCTION

With rapid development of the Internet, E-commerce is becoming an important commerce pattern. How to offer more personality service and how to improve customers' satisfaction to the website, witch is an important problem every businessman has to solve. Fortunately, recommender system in e-commerce just is a best way of all. Recommender system is a kind of individual information filtering technology, and it is also a synthesis of the knowledge or technique of Statistic, Artificial Intelligence, Data Mining and Psychology. It can forecast user's interest by analyzing his visiting behaviors.

Now there are many examples of recommender applications in the world, such as recommending products at Amazon.com . At the same time, many scholars develop a great deal of new approaches on this research area, for instance content-based recommender algorithm, rule-based recommender algorithm, collaborative filtering recommender algorithm, and so on. Collaborative Filtering is one of the most important algorithms among them, and it is used both in the industry and academia widely.

Computation bionics is becoming a study hotspot on the research area recently. It can be used to solve some special problems or to improve existent algorithms, and both of them are all very successful. Specially, how to make some existent algorithms more intellective by introducing the theory is the study emphasis now.

The work is based on Steve's study (Steve & Uwe, 2002), and we present two methods to improve his algorithm. The experiment result shows our methods enhance its whole capability. The remainder of this paper is organized as follows: In the next section, a very brief overview of the immune system is given with particular emphasis on those features that we intend to exploit here. And we also introduce some basic knowledge of collaborative filtering recommender algorithm. Section 3 wills describes our methods in detail. The following section shows and analyses our experiment result.

2 OVERVIEW OF THE BASE ALGORITHMS

2.1 Artificial Immune System

The human body is protected against foreign invaders by a natural immune system. The AIS (Artificial Immune System) is inspired by it, through building a set of distribution system to solve some difficult problems in the real world.

The immune system has a lot of features, such as antigens recognition, diversity, distribution, self-organizing, etc. (Tao Li, 2004). Antigens identifying means the measurement of relativity of antibodies and antigens. Diversity means antibodies exist dispersedly in the whole antigens' space, hence only a few antibodies can recognize vast antigens. Distribution means there is not a central supervisor of the whole system, but each part is an independent unit. Self-organizing means immune system can adjust itself to a new balance state when the old balance state has been broken because of some new antigens.

The idiotypic network theory, introduced by Jerne in 1976 (Jerne, 1974), maintains that interactions in the immune system do not just occur between antibodies and antigens, but that antibodies may interact with each other. Hence, an antibody may be matched by other antibodies, which in turn may be matched by yet other antibodies. This activation can continue to spread through the population. However, this interaction can have positive or negative effects on a particular antibody-producing cell. This theory could help explain how the memory of past infections is maintained. Furthermore, it could result in the suppression of similar antibodies thus encouraging diversity in the antibody pool.

Farmer set forth his differential equation model of the idiotypic network theory (Farmer, Packard & Perelson , 1986)

$$\frac{dx_i}{dt} = c\left[\sum_{j=1}^{N} m_{ij}x_i x_j - k_1\sum_{j=1}^{N} m_{ij}x_i x_j + \sum_{j=1}^{n} m_{ij}x_i y_j\right] - k_2 x_i$$

(Formula 1)

Where N is the number of antibodies in the network, n is the number of antigens, x_i (y_j) is the concentration of antibody (or antigen), c is a constant, k_1 is suppression, k_2 is death rate, m_{ij} is matching degree of antibody i and antigen (or antibody) j.

Steve and his associates improve Farmer's model, and describe the idea of using immune theory in recommender system. The follow is their amendment equation.

$$\frac{dx_i}{dt} = k_1 m_i x_i y - \frac{k_2}{n}\sum_{j=1}^{n} m_{ij}x_i x_j - k_3 x_i$$

(Formula 2)

Where k_1 is suppression, k_2 stimulation, k_3 death rate, x_i is the concentration of antibody i, m_i is the matching degree of antibody i and the antigen, m_{ij} is the matching degree between antibodies i and j, y is the concentration of the antigen, n is the number of antibodies.

In this model, after each iteration the immune system will adjust the concentration of each antibodies in the network,

according to the antibody and antigens correlation as well as the correlation between the antibody and other antibodies. Finally, those antibodies with lower concentration will be dropped. In this way, it can implement the diversity of antibody network by simulating the metadynamics rule of immune system.

2.2 Collaborative Filtering Algorithm

Collaborative filtering (Goldberg, 1992; Resnick, 1994) is one of most important recommender algorithms. It tries to predict the utility of items for a particular user based on the items previously rated by other users. It selects the users that have the same interest with this user as references. The key of this algorithm is how to get more accurate neighborhoods of the active user.

The main steps of this method are: (Emmanouil, 2003)

1. *Representation*. The input data is defined as a collection of numerical ratings of *m* users on *n* items, expressed by the *m*×*n* user-item matrix.
2. *Compute Similarity Value*. Confirm the distances computation function between two users, and get their correlation value.
3. *Neighborhood Formation*. Generate the active user neighborhoods based on his correlation value with each other.
4. *Prediction.* Select appropriate prediction function and use one item rating of the active user's neighborhoods, to get the item prediction rating for the active user.
5. *Recommendation Generation*.

Whether the correlation value is exact or not is the key of this method, because it will affect the recommendation quality directly. We use Pearson Correlation (Resnick, 1994) in this work.

$$sim(x,y) = \frac{\sum_{s \in S_{xy}} (r_{x,s} - \overline{r_x})(r_{y,s} - \overline{r_y})}{\sqrt{\sum_{s \in S_{xy}} (r_{x,s} - \overline{r_x})^2} \sqrt{\sum_{s \in S_{xy}} (r_{y,s} - \overline{r_y})^2}}$$

(Formula 3)

Where S_{xy} is the items which are valued by both user *x* and *y*, $r_{x,s}$ is valued by user *x*, $\overline{r_x}$ is the average value that user *x* gives for all items.

The Prediction Function is:

$$P_{x,i} = \overline{r_x} + \frac{\sum_{y=1}^{n} sim(x,y) \times (r_{y,i} - \overline{r_y})}{\sum_{y=1}^{n} sim(x,y)} \quad j \le n$$

(Formula 4)

Where $P_{x,i}$ is the prediction result that user *x* values to item *i*, *n* is the number of neighborhoods of user *x*.

The essential of recommendation algorithm is how can grasp user's interest exactly and make an appropriate decision. The basic demand of CF algorithm is acquire a set of "perfect" neighborhoods. Here "perfect" means neighborhoods can represent all interest area of the active user by and large. So how to make effects to enhance the diversity of neighborhoods should be a main purpose to improve.

The idiotypic artificial immune network has some outstanding advantages on lots of aspects. Therefore we can take advantage of this theory when we want to find neighborhoods of the active user. In this way we can get a set of more diverse neighborhoods. The active user can be seen a antigen, and others which have been in this system can be seen antibodies. We can find neighborhoods of the active user by building a stable antibody network. In this network antibodies are able to identify the antigen, on the other hands there are a few of obvious distinctions among them. So this network is diverse.

3. OUR ALGORITHMS

Steve and his associates gave a recommender method based on immune theory in 2002 (Steve & Uwe, 2002). Their algorithm can deal with user's diverse interest, and it can achieve better prediction result. But it has a serious shortcoming that is bad performance. Their algorithm must do many complex calculations to form the antibody network for each active user. Therefore, with the number of users increasing, its complexity will go up in exponential growth.

We try to improve it on two aspects:

First, Clustering Immune Network Recommendation (CINR). With clustering technique, we divide it into off-line modeling phase and on-line recommendation phase.Second, Parallel Immune Network Recommendation (PINR). With parallel technique, we shift it into a kind of parallel algorithm.

3.1 CINR

The algorithm has four steps:

1. Apply K-means clustering algorithm to group the users. (Off-line modeling phase)
2. Use those center users of groups as candidate neighborhoods for the first iterative calculating.
3. We select several center users from these candidates, and combine these groups into a big user aggregation.
4. Apply the algorithm on the new user aggregation again, and get the final neighborhoods of the active user.

Main procedure:

```
Apply K-means clustering algorithm to group the users
    //off-line calculating
Initialize AIS with the centers of groups
Encode user for whom to make predictions as antigen Ag
WHILE (Reviewers available)                    //S
    Add next candidate neighborhood user as an antibody Ab
    Calculate matching value between Ab and Ag
    Calculate matching value between Ab and other antibodies
    Set all antibodies to initial concentrations
    WHILE (Don't finish iteration calculation)
        Iterate AIS
    END WHILE
    Delete the Ab with lowest concentration
END WHILE                                      //E
Get K (K<<N) centers are similar to the active user
Combine these K groups into a new user aggregation (size is L),
and initialize AIS
Apply step S~E again, and get the final neighborhood
aggregation (size is m)
```

The analysis of algorithm complexity:

Our focus is algorithm's response time, so we will analyze on-line phase mainly.

Suppose *N* is the number of neighborhoods, *n* is iteration time, *m* is the size of AIS.

The time complexity of Steve-algorithm is: $(N-m)\times(2m+n\times m\times m)$. With notation *O* (Gilles, 2003), it

is an algorithm of $O(Nnm^2)$.

The time complexity of CINR is:
$(K-m+1)\times(2m+n\times m\times m)+(L-m+1)\times(2m+n\times m\times m)$. Because *K* is less than *L* generally, it is an algorithm of $O(Lnm^2)$. Furthermore, *L* is far less than *N*, so its on-line response time is far better than Steve-algorithm.

3.2 PINR

In Steve-algorithm, the main operations are iteration calculations, and each step is independent of other steps. Hence, we apply parallel technology to rebuild Steve-algorithm.

Main procedure:

```
Group all candidate neighborhood users (K subgroups,
Tlen users in each subgroups )
Encode user for whom to make predictions as antigen Ag
WHILE (Reviewers available)
    Add a group of candidate neighborhood usesr as
antibodies Abs
    Initialize an array V[All], each item of the array stores
matching value of an Ab and the Ag (All= Tlen+ SizeOfAIS)
    Initialize another array M[All][All], each item of the
array stores matching value of an Ab and other Abs
    Process of Each Ab In Parallel          //S1
        Calculate matching value between Ab and Ag,
    store in V[All]
        Calculate matching value between Ab and other
    Abs, store in M[All][All]
    End Parallel                            //E1
    Synchronize all sub-processes
    Set all antibodies to initial concentrations
    WHILE (Don't finish iteration calculation)
        Process of Each Ab In Parallel      //S2
            Iterate AIS
        End Parallel                        //E2
        Synchronize all sub-processes
    END WHILE
    Delete the Abs with Tlen lowest concentrations
END WHILE
```

The analysis of algorithm complexity:
Steve-algorithm is an algorithm of $O(Nnm^2)$.

The time complexity of PINR is:
$(K-m+1)\times(1+All+n)$, $All=Tlen+n$. It is an algorithm of $O(Kn)$. (Step *S1~E1* and *S2~E2* are running in parallel, so their time complexities are both 1.) Furthermore, *K* is far less than *N* and the algorithm is foreign to the size of AIS (m), so PINR is a kind of algorithm with very fast response speed.

4. EXPERIMENTS

4.1 Dataset& Evaluation Metric

In order to execute the experiments of this work we used the original GroupLens data set (MovieLens). The data set consists of 10,000 ratings, assigned by 943 users on 1682 movies. All ratings follow the 1(bad)~5(excellent) numerical scale and each user was required to express his opinion for at least 20 movies in order to be considered.

We choose MAE (Mean Absolute Error) as our evaluation metric. The metric is used to measure the accuracy of prediction usually. (Herlocker, 1999)

$$MAE = \frac{\sum_{i=1}^{n}|p_i - r_i|}{n}$$

(Formula 5)

Where p_i is predicted value, r_i is actual value, *n* is the number of predictions. Better recommender algorithm's MAE is lower.

4.2 Result Analysis

Experiment 1:Compare the accuracy of five algorithms.
All of the results are got in this environment: Windows2000SP4, CeleronIV 900M, 128MB Memory, J2SDK_1.4.2.

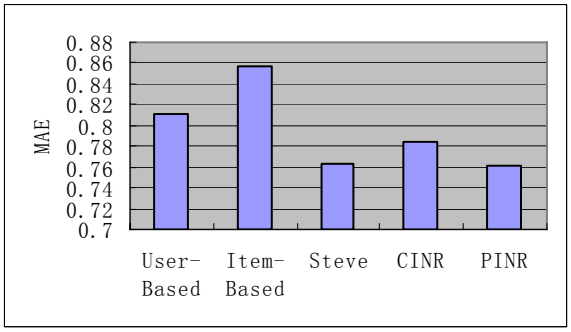


Fig.1. The average MAEs of five algorithms

Fig.1 shows the average MAEs of five recommender algorithms. From this chart we can find those algorithms which basing on immune theory are more accurate than two traditional methods. This result proves that it is very important to build a proper model to show user's diverse interests. Otherwise, PINR's and Steve-algorithm's MAE value are almost equal, but CINR's MAE value is higher. Maybe, the reason is that clustering operation makes CINR algorithm losing a few of potential neighborhoods, therefore failing to grasp one user's interest accurately.

Experiment 2:Compare the responses time of two algorithms.
All of the results are got in a Linux Cluster wih 8 PCs.
The configurations of Linux Cluster with 8PCs are as follow:
The configurations of Master Server (acts as Slave Node at the same time):Fedora Core 5, Pentium IV 3.0G, 512MB Memory(DDR), mpich-1.2.7. The configurations of 7 Slave Nodes is Fedora Core 5, Pentium IV 3.0G, 512MB(DDR) Memory(named Type A, 2 PCs in all)

We use single PC(Master Server) in Steve-algorithm, two PCs (Master Server and a Type A PC)in PINR(2), four PCs(Master Server, 2 Type B and a Type C PCs), and 8 PCs(Master Server and all Slave Nodes).

Fig.2 shows the responses time of two algorithms. Specially, response time of Steve-algorithm is a standard score (value is 1). From this chart, we can see PINR(2) is worse than Steve-algorithm, but PINR(4) and PINR(8) are both better than Steve-algorithm, especially PINR(8). The reason is that the increasing communication time is longer than the decreasing computation time in PINR(2). We have already made extra experiment to prove it. Since the extra experiment is beyond the scope of this paper, it is not necessary to present the result in detail. Because of the obvious better result in PINR(4) and

PINR(8), We can make the conclusion that Steve-algorithm is suitable for paralleling. In addition, comparing the responses time of PINR(2), PINR(4) and PINR(8), it is decreasing. We can predict that if we use 16 or more PCs in cluster, the result will be better.

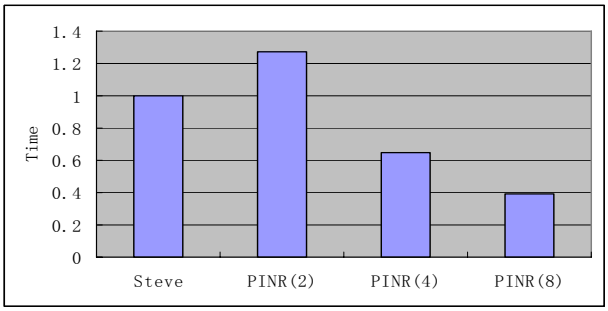


Fig.2. Responses time of two algorithms

5. CONCLUSIONS & FUTURE WORKS

It is a hot issues that applying ecological system algorithm (such as immune theory and ant colony algorithm et al.) into computation area now. How to make suitable model to show the biological characteristics better and to resolve real problems is the kernel of these researches. In this paper we study the immune theory in depth and bring up two improved algorithms based on the works of Steve et al. We gain relatively desirable results in experiment. In the future we will make an effort to optimize the algorithm at following two aspects. Firstly, establish a computer-cluster and transplant PINR into a real parallel environment. Secondly, enhance CINR algorithm with demographic data to get better clustering effects.

REFERENCES

[1] Emmanouil Vozalis, Konstantinos G. Margaritis (2003), “Analysis of Recommender Systems’ Algorithms”, HERCMA.Farmer JD, Packard NH and Perelson AS (1986), “The immune system, adaptation, and machine learning,”in *Physical*,vol.22,pp.187-204.

[2] Gilles Brassard, Paul Bratley (2003). Fundamentals Of Algorithmics. Pearson Education: USA.Goldberg, D., Nichols, D., Oki, B. M., and Terry, D (1992), “Using collaborative filtering to weave an information tapestry,”in *Communications of the ACM*,Vol.35,pp61-70.

[3] J.Herlocker, J.Konstan, and J.Riedl (1999). “An algorithmic framework for performing collaborative filtering,”in *ACM-SIGIR Conf*,pp230~237.

[4] Jerne N K (1974). “Towards a Network Theory of the Immune System,”in *Annual Immunology*,vol.125c.

[5] Resnick, P., N. Iakovou, M. Sushak, P. Bergstrom, and J. Riedl (1994).”GroupLens: An open architecture for collaborative filtering of netnews,”in *Proceedings of the 1994 computer Supported Cooperative Work Conference.*

[6] Steve Cayzer, Uwe Aickelin (2002). “A Recommender System based on the Immune Network,”in *Proceedings CEC2002*,pp807-813.

[7] Tao Li (2004),*Computer Immunology*,Publishing House of Electronics Industry: China.

The Inheritance Abnormal Problem of Component Parallel Evolution

SenYang, Qing Liu
Yunnan University
KunMing, Yunnan Province ,China
Email:yang82101@163.com

ABSTRACT

The component evolving has important meaning to component reusing. The feature of erupt make the component evolving involve to the erupting object's inheritance abnormal problem. Commence from a relation of component in this text, we discuss some problem which about the inheritance and synchronization in component evolving. Carrying on analyze which about the abnormal problem in component evolving commences from development pattern. Then a special interface is the rule to avoid inherit abnormal phenomenon.

Keywords: Component, Inheritance Abnormal Problem, Evolving-Interface

1. INTRODUCTION

In the component software system, component erupts naturally as the basic unit. The feature of erupt happened inside the component and outside, it have the relationship of synchronization code. Synchronization code constructs the synchronization constrains erupt of activity between the interface and component insides. Carry evolving functions on to thus components that the existence erupts (the interior or exteriors erupt) feature probably must to modify the original code. Then the synchronization constrains would be destroyed. The component will become so difficult to reusing. Holding to the inheritance abnormal phenomenon from the essence is basic path that resolves this problem.

2. THE ABNORMAL PROBLEM ABOUT COMPONENTS EVOLVING WITH THE INHERITANCE MECHANISM

2.1 The Principle of Software Evolving

Along with the development of technique and demand, the software system needs to carry on sustain then in its life cycle of improvement. The software system is becoming more and more mature along with the frequency of improvement becoming higher and higher. Then this improvement can be described as "software evolving".

2.2 The Component Evolving Mode

The components are developed to catch the need of different demands, and according to the different hypothesis of the context The component usually must be rewrite while applying to a new system, the component that is rewired becomes a to an another version. The degree to the comprehension of component structure comes to different way to component evolving [1].

1) Write box method. The user can get all code of this component, so component rewritten make it can operator with the others. This method must modify the source code, so it will bring in serious problem about maintenance and upgrade, losing many advantage the component software have.
2) Black box method. We can get the binary application form of component only. The component did not provide to expand the mechanism or API.
3) Ash box method. The component provided it with the extension mechanism or programmable interfaces of the oneself, but the source code of this component can't be modified directly.

2.3 The Abnormal Phenomenon In Component Evolving With Inheritance Mechanism

The inheritance is a kind of hierarchy relation of the classes. Generally, the class hierarchy can be seen as a kind of type hierarchy in the Object-Oriented programming language. Then the relation of super class and sub class is the same as the relationship between super type and sub type. The software which oriented to component beyond to Object-Oriented software[2], so the component software must be invoke the inheritance abnormal problem when evolving with the heritance mechanism. The abnormal problem of inheritance not only be brought in the OO SE in the general meaning, but also brought some to component and structure as the component evolving.

3. THE INHERITANCE OF THE COMPONENT INTERFACE

We should pay more attention to the interface than the detail of component in the integration of the component. The interface is the unique path of exterior and components, so the component evolves can be seen as the interface evolving. The component evolving with inheritance method will be expressed the inheritance of interface.

3.1 Interface Specification

A kind of valid interface specification method is the contract of the interactive procedure between the client and the server interface.The contract describe the state of client claim the server first, then describing the state that the server port carry the service. The client port established the precondition

before requesting service, service port satisfied the client request with internal logic depended on the precondition. The service port must established the postcondition before giving feedback to client and the client got the service by the postcondition[3].

The specification of interface is two tuples on the hierarchy of the contract:
IF :=< precondition ,postcondition >
This condition expression shows the behavior of the interface:
precondition ⟶ postconditon

Next is a proof that component behavior equal to condition operator:

Table 1 component behavior equal to condition operator

precondition	postcondition	Precondition ⟶ postcondition
T	T	T
F	F	T
F	T	F
T	F	F

These values match the feature of condition operator, so the specification of the interface function is a condition expression:

Precondition ⟶ postconditon

3.2 Distinguish the Inheritance Hierarchy as Component Evolution

The interface is unique interactive medium of the component and exterior, the component reusing and evolution depended on interface, so any studies about component evolution with inheritance mechanism should be start at the heritance of interface.

In the OO theory, inheritance had two hierarchies: inheritance and sub typing[3]Inheritance made the modify on the code hierarchy while the subtyping makes the modify on the semantics hierarchy. The former is a important way of code reusing but can't guarantee that the subclass can inherit the super class's behavior; the latter requests a certain exterior of the subtype hold supertype and can be observe the behavior(or the semantics behavior), in one stage share of norm. In another word, we should pay more attention to the semantics reusing but the reusing of code.

Now we can specializes the component as these triple forms:

C :=< CDS, IF , CR >

C: component

CDS: component description

CR: component relationship

IF: interface

So the relationship of C1, C2 can be express as following from:

C1= C2 ⟺ CDS1 = CDS2 ∧ IF1 = IF2 ∧ CR1=CR2;

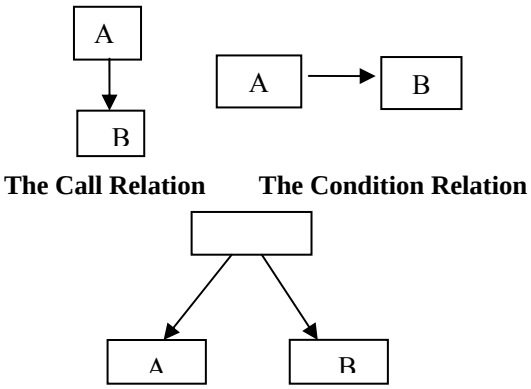
Then the component's code can't identify itself, inherence in component hierarchy should be modify of semantic. Concreting to the semantics of the interface, it can be seen as the inheritance of the condition expression:

precondition ⟶ postconditon

4. DEFINE THE ABNORMAL PHENOMENON OF COMPONENT INHERITS

4.1 Algebras spaces of the component operation

As the description in thesis[3], the operation among components mainly has these following kinds:



The Call Relation **The Condition Relation**

The Cooperation Relation

Fig.1. The component operation

The operation among components is carry out by the interface in fact, according to thesis[3],it can be specialized into interface hierarchy:

C1.IF: A1 ⟹ B1; C2.IF: A2 ⟶ B2

Calling: C1 * C2 ⟹

A1 ∧ A2 ⟶ B1 ∧ B2

Condition: C1 ⟶ C2 ⟹

A1 ⟶ B1 ⟶ B2

Cooperation: C1 + C2 ⟹

（A1 ⟶ B1 ）∧(A12 ⟶ B12 ）

In parallel environment, the component operation essence can be seen as the operation of the Boolean expression of component interface[4].

The express "IF < precondition, postcondition >" is a specification of interface. Then dom（IF）, ran (IF) ∈I∪ Z , the I is a space inside the component, the Z is a space outside the component.

4.2 The Essence of Inheritance Abnormal Phenomenon in Component Parallel Evolution

If operation ▲ followed the rule of component construction and the interfaces

"IF<A , B>"which take part in the operation take the value as ①A, B∈I∪ Z, ②C1 ▲ C2 = TURE, these component can be constructed. As the description of thesis [1], component status which lives inside can't be seen outside. Then the filed of interface which take part in the operation only should take the value as 'Z'.

Now, the specification of the interface semantics became the following form:

IF ＜λ∧A, μ∧B＞, λ , μ ∈I; A, B ∈ Z;

IF : λ∧A ⟶ μ∧B;

We can change the component operation into the following form by mathematic principle:

C1 ▲ C2=f (A, B) ∧ ϕ(λ , μ)

f (A，B): Boolean expression with the relationship of A, B

ϕ(λ , μ): Boolean expression with the relationship of λ , μ

The traditional definition concealed the existent fact of the φ (λ, μ) factor in component operation, so the internal semantics (state) of the component to was neglected. The complete of the component development process guaranteed that the φ (λ, μ) always is true, but as the evolution of component happened, the interface evolution will make the φ (λ, μ) evolve more or less. If that happened, the value of φ (λ, μ) may change into FALSE. Now guarantied φ(λ, μ) always had a value of true is a key job that don't exist in demand declaration but decided the future of this system.

When component evolution carried out in parallel way, for example, there are two components C1, C2, them evolved at the same time, the operation becoming the following form:

C1'▲ C2' = *f* '(A', B')∧(ϕ1(λ1, μ1) ▲ ϕ2(λ2, μ2))

Then we must conjunction the evolution of the C1, C2 internal semantics(φ1(λ1, μ1), ϕ2(λ2, μ2)) together. But the less coupling and encapsulation of component decision:

(1) It is difficult to get the internal semantic of component or this function is very difficult.
(2)The phenomenon of the evolution in one component making other evolutions happened in the other components will destroy the performance of the strut.

Then the right way to solve component inheritance abnormal is the improvement of modeling principle in component development.

5. THE WAY TO AVOID THE INHERITANCE ABNORMAL PHENOMENON

5.1 The Definition of the Evolving-Interface

The affliction between internal-semantic and external-semantic brings out the inheritance abnormal phenomenon. The internal-semantic is encapsulated in traditional SE theory, so any work to remove these afflictions can't success at all. Today the software process should support evolution-software-process; the evolving-interface must be added into component to support the evolution-software-process. This interface contains some calling-back methods that had strict defined by the extent of evolution and the right of modify.

5.2 Separate the Internal Semantics

According to the former description, the component semantics can mean with the Boolean expression Σ at last. Then Σ can be change into the following form:

Σ = *f* (A, B) ∧ ϕ(λ, μ)

The task of evolving-interface is guarantee ϕ1(λ1, μ1) ▲ ϕ2(λ2, μ2) had a value of true. Now the granularity of the φ (λ, μ) still too greatly, modify the component semantic wholly disobey the principle of component evolution. We need to divide ϕ (λ , μ) into two parts: The nucleus semantics – α;the extension semantics --β. Then'α' can't do any changes at all while 'β' can be modified.

The φ (λ, μ) can change into the conjunctive normal form by mathematic principle:

$$\phi(\lambda,\mu)=\underbrace{\omega 1\wedge\omega 2\wedge\omega 3}_{\alpha}\wedge\underbrace{\ldots\wedge\omega n}_{\beta}$$

Thus, the internal semantic which evolving-interface can influence contained in β . α can't be evolved at all. The evolution is carried by the principle of the basic semantics of component mustn't be changed. Suppose the occurrence of inheritance abnormal namely the semantics conflict probability presents the normal distribution. The α , β can be divided as the form which showing in following graph to guarantee the efficiency of the interface:

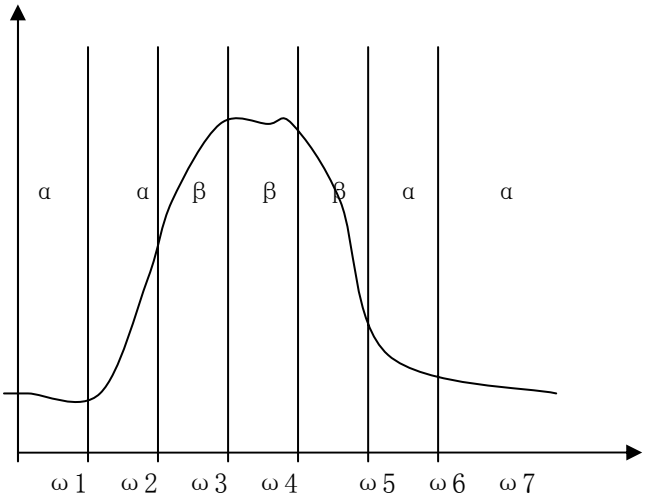


Fig.2. The Divid way by semantics of component

5.3 The Work Method of Evolving-Interface

When the inheritance abnormal problem happened, ϕ(λ , μ)= α ∧ β and
β =FALSE. The work of evolving-interface is with a factor σ and β to make the operation. Then β ▲ σ =T. Thus ϕ(λ , μ)= α ∧ (β ▲ σ) always has a value of TURE. Usually there are two kinds of operation methods:
(1) Establish the σ = T, make the β∨σ = T;
(2) β ⟶ σ = T;
The σ is a Boolean expression, it's concrete form according to the evolve demanding. If ζ can operate with the precondition to get some postcondition to The consistency of the internal semantics and the function interface semantics. Then factor ζ is called evolution-pattern-factor.

The specification of evolving-interface likes the following form:
IFE: = 〈 β ∧ ζ , β ▲ σ 〉
The functional specification is:
IFE: β ∧ ζ ⟶ β ▲ σ . ▲ can be any combination of Boolean operation.

When then component evolving, evolution process call the callback-function to evolve the internal semantic of component by parallel way. Generally speaking, every related internal semanticist all need to use the evolving-interface to the consistence of internal semantic and exteriors to prevent from the occurrence of inherit abnormal phenomenon.

6. CONCLUSIONS

The occurrence of inherit-abnormal-phenomenon is the conflict between the internal semantic and exteriors. In my paper, I try to get a mathematic way to release this phenomenon. Through the component operation of a series, the inherit-abnormal-phenomenon can be solved by making

the internal semantic and exteriors got a same value.

In the future, we need to modeling to internal semantic and exteriors of component delicacy. Then make the component software process support evolution. Making component can with a kind of unify of evolution- process model development.

REFERENCES

[1] Pierre America, "A parallel object-oriented language with inherence and subtyping," *SIG-PLAN*, 25(10):161-168, October 1990.

[2] Clemens Szyperski, Dominik Gruntz StephanMurer, *Component Software: Beyond Object-Oriented Programming*, Publisher of electronic industries,2004.

[3] Zhang You Sheng, "The Component Operation and Software Evolves Research," C*omputer-Application*, Vol. 24, No. 4.

[4] Medvidovic N, Taylor RN, "A Classification And Comparison Framework for Software Architecture Description Languages [J]," *IEEE Transaction on Software Engineering*, 2000, 26 (1): 70 - 93.

Design the Library of Search Algorithm Based on Design Patterns

Luo Zhong, Juan Fu, Wei Zhang, Maolin Wang
School of Computer and Technology, Wuhan University of Technology
Wuhan, Hubei, 430070, China
Email: vanilla_fu@163.com

ABSTRACT

At present search algorithm are designed by the concrete question, it has to redesign when used in other area. It is not only waste time and money, but also not assure the accuracy of search algorithm .Because of that, this paper designs the library of search algorithm by design patterns based on analyzing many search algorithm. The library of search algorithm based on design patterns independent from the concrete application, and it is effective solve the development of search algorithm.

Keywords: AI, Design Patterns, Template Method, Search Algorithm, Algorithm Library

1. INTRODUCTION

The main contents of AI (Artificial intelligence) research include: problem solving, logical reasoning, theorem proving, machine learning, knowledge acquisition, knowledge processing systems, natural language understanding, computer vision, automatic programming and so on. Although there are a number of artificial intelligence research fields, and each field of research also has its own rules and characteristics, it can be abstracted as a process of problem solving from the process of they solve practical problems .After analyzing the use of artificial intelligence research in the problem-solving methods, it can be found that many methods obtained the solution of problem by search. So the process of problem solving can actually be seen as a process of search.

Now, search technology is wildly applied in the different kind of AI systems. Such as expert systems, natural language understanding, automatic programming, pattern recognition, robotics, information retrieval and Game and so on. Although the search has already been extensive development, most of the people care the search efficiency of search algorithm, that is means how to improve the algorithm to enhance the search efficiency, and it be not pay attention to the intrinsically relation and related research between various search algorithms. And then, the search algorithms are concerned in the application of a concrete domain or problem, in other words, that is concerned how to design and implement search algorithm to solve the problem. However, in practical application, the same search algorithm can be applied to many problems, search algorithm is designed only to consider the current application areas, it led to the current search algorithm is designed to the problem with excessive dependence, and it has to re-design when using search algorithm in different areas. It can be caused repetitive work, and the design of the search algorithm is less universal.

2. SEARCH ALGORITHM AND DESIGN PATTERNS

2.1 Search Algorithm

There are two kinds of search algorithm, blind search and heuristic search. Blind search also named no-info search, which only search under the search control strategy set before in the search process. Blind search is blindness, low effect and not convenient in work out the complex problem because of it always run in the route set before and not consider the characters of the problem itself. Heuristic search also named info search in which add heuristic info related with the problem and change or adjust the search direction in the search process. It is make the search run in the most hopeful direction, speed up the problem solving and find the best answer at last. Although heuristic search consider the characteristic of the problem and use it to rise up the efficiency of problem solving, also make it easier to work out complex problem, but it not convenient to abstract the characteristic and info of all the problems. So even heuristic is better than blind search, blind search is still a search strategy used a lot.

2.2 Design Patterns

The early 90s of the 20th century，some smart software developer occasional found architect Alexander’s research about pattern, which transferred design patterns from architecture to software. Design patterns bring forward a universal design solve scheme and give it a systemic name and dynamical explain aim at the design problems repeat arise in the object-oriented system, It is a set of coding design experience conclusion which is repeating used、most people known、classified. Design patterns’ basic thought is separate the part which is likely to change from the part which is not change in the programming, try to induce the coupling between the objects, so when some object changed, it would not lead to the full change of the other objects. In order to realize this aim, a common method used in pattern is to add a middle classes or objects during the classes or objects. This would make the code extend and maintenance easier and also make the programming read easier.

3. THE STRUCTION OF THE LIBRARY OF SEARCH ALGORITHM BASED ON DESIGN PATTERNS

According to the thinking of design patterns, the structure of the entire library of search algorithm can be designed as showed in Fig.1. The bottom layer primarily is responsible for implementing public operations, namely, the public interface of the function and class. It is mainly service for implementing the search algorithm in the second layer. However, it is considered the current search algorithm realized is only a small part of the large search algorithm, not covers all search algorithms. So the bottom of the interface functions and classes open can be help for the later developers develop the search algorithm to meet their demand, and make it more efficient. It also can be used by the higher level developer. This greatly increases the library of practicality and software reuse. At the same time, these interfaces also can provide not only for the developers to use, but also the higher level of users to call search algorithm. The bottom set of operation contain public operations and relative

data structure. It is surely the library is only include a certain amount of algorithm, in order to maintain the algorithm library in the future, the bottom of these interfaces is also provided for use by third parties, it can expand the search algorithm, which includes more search algorithms.

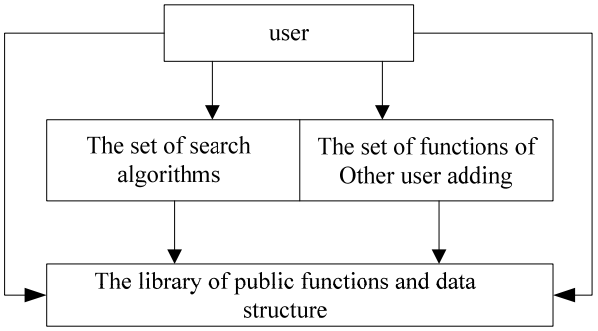


Fig.1. The structure of the library of search algorithm

4. ANALYZING THE SEARCH ALGORITHM

State space search for the basic process, the flow chart show in Fig.2:

(1) Establish the search graph G which only contains an initial node S_0, and then S_0 Add into the OPEN table.
(2) Establish the CLOSED table, and set to an empty table
(3) Judge OPEN table whether is empty, if empty, the problem is no solution, failure and exit
(4) If the OPEN table is not empty, pick up the first node of the OPEN table, and add in the CLOSED table, this node name as n.
(5) Judge N whether is the target node, and if it is, the problem has solution, success and exit. the solution of problem is the path from the graph G along pointer from n to the S_0
(6) Expand n, if its children aren't subsequent nodes of n's ancestors, and name them as set M, put M's nodes into graph G as the Subsequent nodes of n
(7) The nodes of M have been appeared in seen in the G, but are not in the table of OPEN or CLOSED, set a pointer to the father node (node n), and add these nodes into OPEN table; for those have been seen in graph G, determine whether it is need to modify pointer to the father nodes (node n) of the target; for those who have previously G and the CLOSED table, determine whether they need to amend the pointer to subsequent nodes.
(8) Re-sort the nodes of the OPEN table by a certain method or strategy
(9) Go to the third step

Blind search and heuristic search can be seen as a special case of state-space search. The main difference between of all kinds of search algorithm is the ort algorithm of the nodes in the OPEN table. If the sort of the OPEN table is random or blind, the search is blind search. If the sort of the OPEN table is based on heuristic information or rule sorting criteria, it is heuristic search.

The difference between BFS (breadth first search) and DFS (depth first search) is the position of the next sibling in the OPEN table when extending the node in blind search. The strategy dealing with the nodes in the OPEN table in BFS is FIFO and that in DFS is LIFO. OPEN table in BFS is a queue and that in DFS is a stack. In heuristic search, the difference between A and A-star algorithm is the different Cost Functions used to sort the nodes in OPEN table.

Bounded DFS is improved from DFS. Comparing with the DFS, BDFS limits the searching depth of the node in OPEN table. In terms of searching algorithm, we can understand the relationship between blind search and heuristic search as following: Heuristic search is improved on base of blind search to enhance the searching efficiency. The more basic the algorithm is the less data and knowledge needed. The more complicated the more knowledge and data needed to develop the efficiency and avoid searching the useless nodes. So we can draw a conclusion that heuristic search is a developed algorithm that adding estimate-factor to blind search to decrease the searching times.

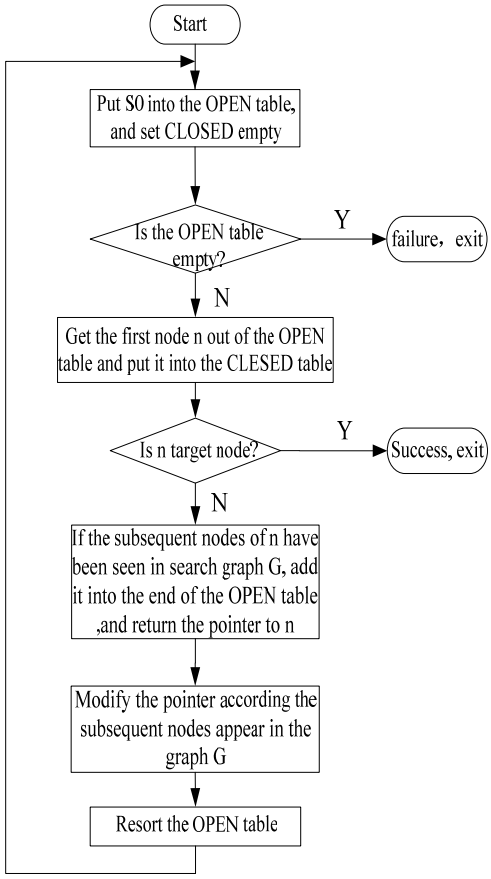


Fig.2. The base flow chart of state-space search

5. THE DEDIGN OF THE LIBRARY OF SEARCH ALGORITHM BASED ON DESIGN PATTERNS

5.1 Template Method

Design Patterns contain 23 kinds of basic design patterns, including three categories: 1. Creational: abstraction of the process of class's instantiation of 2. Structural: combine class or object together to form larger structures 3. Behavioral: class or object is how to interact and distribute duty. Template Method is a type of design pattern of Behavioral. Template Method defines an operation structure of an algorithm, and some of the operations will be defined in the subclass. Template Method makes subclass can not change the structure of an algorithm can be re-definition of the algorithm of a certain some specific steps. Its structure is shown in Fig.3:

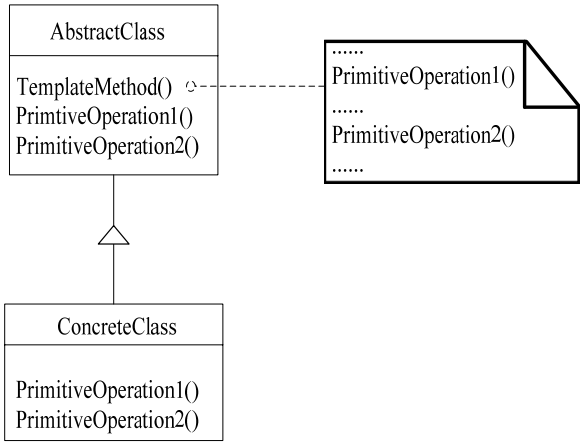


Fig.3. the structure of Template Method

1) AbstractClass : define one or more abstract operations, so that the subclass can be implement; and it define a logical top frame, the logical top component operation is in the corresponding abstract operation, it will be deferred to implement in the subclass.
2) ConcreteClass: realize one or more abstract function which AbstractClass define, they are a logical top component operation; each role of AbstractClass can have any number of corresponding role of ConcreteClass, and each role of ConcreteClass can implement the different abstract methods.

5.2 The Design Of The Library Of Search Algorithm Based On Template Method

Based on the above analysis, the basic operations of search mainly include: graph update , the operation of the OPEN stable which contain judging whether the OPEN table is empty ,getting the first node to expend ,adding the new 生成的 nodes into OPEN table, and sorting the nodes of the OPEN table. After extraction, the public operate will be defined in the base class, it can be seen in the Fig.4. The figure show that while implementing of the specific search algorithm, such as BFS, DFS and A* search algorithm, it is necessary to design one by one, it is only overload the different operation in subclass.

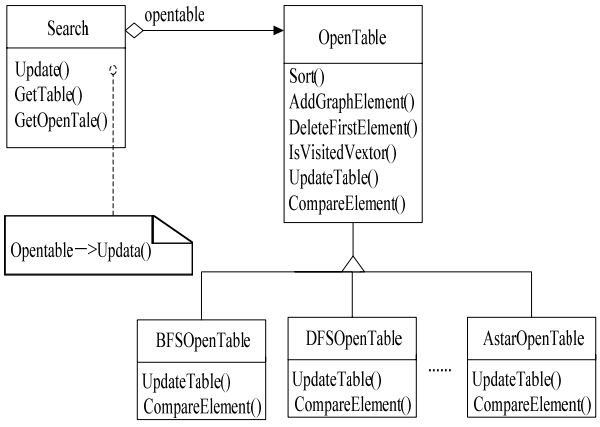


Fig.4. the basic class diagram of the library of search algorithm

6. CONCLUSIONS

In this paper the process of search algorithm design is independent from the specific application areas, it solves the redesign problem causing by the design by depending concrete problem. The search algorithm library designed by design patterns is not only to efficiently improve its universality, expansibility and maintenance, but also to accelerate the pace of design and improve software quality. The universal library search algorithm will satisfy the needs of many areas called search algorithm, and will have good application in the future.

REFERENCES

[1] Nils J.Nilssion, *Artificial Intelligence[M]*, Beijing: China Machine Press, 2000.
[2] Pan Ai-ming, *Theory and Application of COM [M]*, Beijing: Tsinghua University Press, 1999.
[3] Wang Wei, Zhang Bo, Yin Gan-hua, et al, “Designing and Implementation of Map Symbol Database Based on COM [J],” *Geomatics and Information Science of Wuhan University*, 2002, 27(3):269-300.
[4] Xia Yong-feng, Cao Yuan-da, “Implementation and Design Heuristic Searching Algorithm by Object-Oriented Method [J],” *Microcomputer Development*, 2005, 15(7):11-13.
[5] Mandow, L, Perez de la Cruz, J.L., “Multicriteria heuristic search[J],” *European Journal of Operational Research*, 2003, 150(2):253-280.
[6] Zhou, Rong, Hansen, Eric A, “Breadth-first heuristic search [J],” *Artificial Intelligence*, 2006, 170:385-408.
[7] Kovarsky Alexander, Buro Michael, “Heuristic search applied to abstract combat games [J],” *Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science)* , 2005, 3501: 66-78.
[8] Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides, *Design Patterns:Elements of Reusable Object-Oriented software[M]*, Beijing: China Machine Press,2003.

Luo Zhong is a Full Professor and a tutor of Doctor, a head of the School of Computer Science and Technology, Wuhan University of Technology, the principal of Graphic & Intelligent System, a judge of Nature & Science Fund. He graduated from Wuhan University in 1982 and achieved Doctor’s degree from Wuhan University of Technology in 1995 with specialty of structure. He visited Japan and France as scholar; was awarded many prizes by government and has published a lot of papers in kernel journals, which can be searched partly by EI/SCI/ISTP. His research interests are in intelligent technology, expert system, neural network, software engineering, artificial intelligent, distribute computing, image & graphics and parallel processing.

Juan Fu is a Master and graduated from Wuhan University of Technology in 2004. She majors in computer application. Her research interest is in intelligent technology.

Nesting System for Cutting Stock Problem Based on Distributed Parallel Genetic Algorithm

Wei Yang, Qingming Wu, Qiang Zhang, Huadong Zhao
School of Power and Mechanical Engineering, Wuhan University
Wuhan City, Hubei Province, 430072, China
Email: cdrs@163.com

ABSTRACT

According to the difficulty in solving 2-dimensitional cutting stock problem in industries, the paper declared a nesting system for 2-dimensitonal shapes based on distributed parallel genetic algorithm (DPGA). Firstly, it discussed the structure and realization of DPGA, including the data communication module, the fitness function and detailed operators selecting for the algorithm. Then it introduced the bottom-left nesting decoding algorithm to deal with the polygons arranging. Finally the nesting system based on DPGA is designed and it is proved to be efficient by a calculating sample.

Keywords: Distributed Parallel Genetic Algorithm, Cutting Stock Problem, Nesting System, Nesting Decoding Algorithm

1. INTRODUCTION

The cutting-stock problem means the problem of how to nesting parts with different shapes in stocks with the highest efficiency and least material waste. Such problems exist in manufacturing industries widely as 1-dimensitioanl nesting and 2-dimensitional nesting. In which, the 2-dimensitonal nesting problem is the typical NP-Complete problem and it is difficulty to get excellent solutions by general polynomial approaches.

GA is a fine intelligent computing method presenting to the developing of advanced computer technology, it provides the possibility of achieving approximate solutions. In recent years, Al-Assaf[1] has introduced nesting strategies based allocation of two-dimensional irregular shapes. Chen, J.-C. and E. C. Han[2] has researched a computer-aid cutting-stock system on local searching algorithm. Faina, L and Jiang, J. Q., X. L. Xing[3,4] has attempted to use simulated annealing, PSO and genetic operation in cutting stock problem. Edmund, B., H. Robert[5] has discussed the bottom-left nesting algorithm Heuristic Algorithm for the two-dimensional irregular packing Problem. A. Miguel Gomes, José F. Oliveira[6] introduced a heuristic algorithm for nesting problems. Bean, J. C[7] has introduced a multiple-choice genetic algorithm for a nonlinear cutting stock problem.

The parallel computing technology has rapidly developed as the appearance of high speed network nowadays. Multiple computers could collaborate together to attain higher calculating speed and reduce time distinctly. Fred F. Easton, Nashat Mansour[8] has applied the distributed genetic algorithm for deterministic and stochastic labor scheduling problems. Erick Cant, David E. Goldberg[9] has introduced the theory and practice of parallel genetic algorithms in detail. Zdeněk Konfrst[10] has introduced the theory and practice of parallel genetic algorithms. The paper introduces a distributed parallel genetic algorithm in solving the cutting.

2. STRUCTURE OF PARALLEL GA

2.1. Genetic algorithm realization

The Genetic Algorithm is firstly established by J.H.Holland of Michigan University[11]. It is a complex non-linear optimization method based on random intelligence. The traditional GA is executed as Fig.1.

Besides its fine global searching ability and speedy convergence, the major motivation for the use of genetic algorithms actually is their inherent parallelism. Either such a parallelization scheme aims at speeding up the calculations or it can be applied in order to achieve a vigorous improvement of the generated solutions.

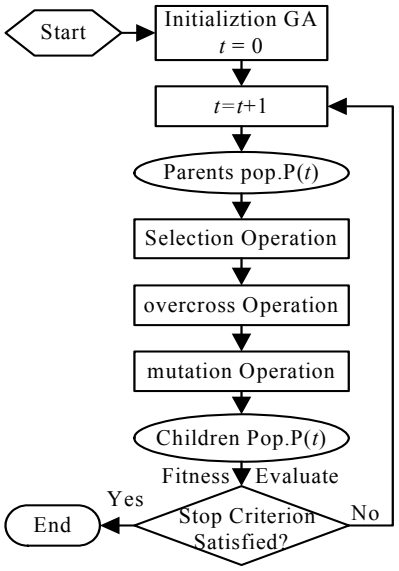


Fig.1. Flow chart of traditional GA

2.2 The structure of distributed PGA

The nature-like parallelization of genetic algorithms mainly contains the following different models: the master-slave PGA model, the distributed PGA model and the fine-grained PGA. The distributed PGA model is also named “the island model”, it is the multiple populations PGA based on a quite loose coupling of their component algorithms and it is more widely researched in general**.** Just subsequent to each lapse of a fixed amount of generations, single selected individuals may migrate to neighbored island populations. Incoming migrants are included into the local populations. Either copies of current individuals (immigration-model) or original individuals (emigration-model), which might have partially spread their genetic material before, are allowed to migrate to neighbors. [8] In the diffusion models there is no need for an explicit migration of individuals. All individuals are considered to move freely within their neighborhood. Thus, the selection operator is no longer limited to the local individuals, but gets access to all neighbored populations, too.

Furthermore, neighbored individuals can be accessed at any time without any limitations. Different to the migration models, only local offspring of neighbored individuals (and no migrants) are included into the local populations.

The distributed system is constituted by series of processing elements. Each processing element has its own independent physical storage component and delay of data transmission among processing elements can not be ignored. Generally speaking, the performance of distributed system is quite restricted by communication and reasonable data communication module design is vital. It is proved that more that more than 90% calculation in GA process is cost by the fitness function, so the paper designed a distributed system based on local area network and distributes the fitness calculation works to different processing elements. Nowadays the local area network is with high dependability in application and the general transmission speed has up to 1000Mbit/s with low delay and bit-error rate. The structure of the distributed PGA model processing is as Fig.2. A central computer is defined to manage the whole optimization function: including island population initialization, computing tasks distribution and information receiving; other computers is defined as satellite computers with the function of genetic operations, fitness calculating and results returning.

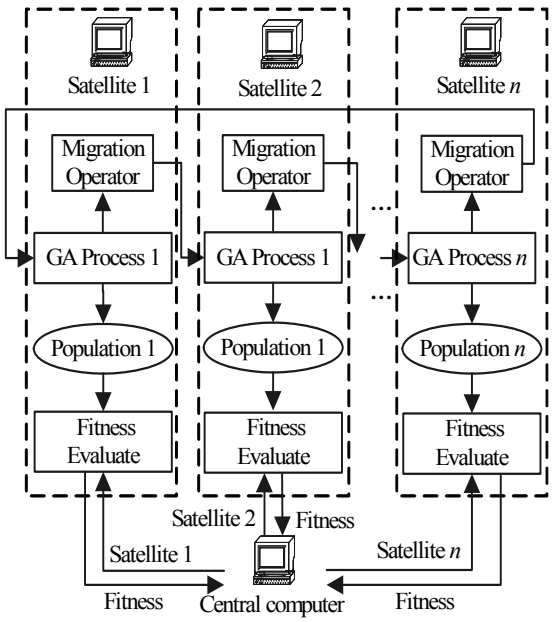


Fig.2. Distributed PGA model(Island model)

3. DETAILS OF DPGA

3.1 The migration operator

The migration operator realizes collaborative evolution of all populations by exchanging information between population islands. In the paper, migration operator is defined to replace the individual with the lowest fitness in the immigration population by the one with highest fitness in the emigration population every 2 generations. And the optimization population is constituted by all the highest fitness individuals in each parallel population. The one with the highest fitness would be the final solution.

3.2 Genetic encoding:

The original binary encoding in solving constrained optimization problem can not meet the need of nesting problem any more. In the cutting stock problem, polygons is described as $P_1, P_2, \cdots, P_i, \cdots, P_n$, the corresponding arranging angles is $\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots, \alpha_n$. The paper defined genetic gene as:

$G_i = [P_i \ \ \alpha_i]$

So the initial individual of the population can be encoded as:

$Individual = Random\ \{Graphic(i)\}|_{i=1\ to\ n,}$ Where:

$Random\ \{Graphic(i)\}|_{i=1\ to\ n}$ represents the random sequence of $Graphic(i) \mid i = 1\ to\ n$ .Such encoding approach realizes the 1 to 1 mapping and it is recommended in genetic algorithm research.

3.3 The fitness evaluation function:

The improved Bottom-left strategy packs all the polygons to the Bottom left corner of the stock at its best. It divides the stock into special columns and arranges polygons from bottom to top in each column. After a column is expired, it will change to another column at the right; and after a stock expired, another stock is changed. According that arranging strategy, the fitness should be related with the total length of all the stocks that has been employed:

$f = \dfrac{1}{\sum_{i=1}^{n} S\text{-}lengths_i}$, Where :

n is the total number of stocks.

$\mathrm{S\text{-}lengths}_i$ is the length of the i-th stock

3.4 Selection operator:

The random selection operator is chose to strength the global optimization ability of the algorithm. Supposed fitness of individual i of the population is f_i and the average fitness of the population is:

$\dfrac{\sum_{i=1}^{n} f_i}{n}$, Where:

n is the total size of the population.

f_i is the average fitness of the i-th individual.

The probability that the individual i produces descendant should be:

$$P(i) = \frac{nf_i}{\sum_{i=1}^{n} f_i}$$

3.5 Crossover operator:

The nesting problem is similar as the Travel Salesman Problem (TSP). So the paper applies the Cycle Crossover (CX) mentioned in [11], which delivers the Cycle Crossover operator is fit for used in solving TSP. The polygons are expressed as vertexes sequence and angles: for polygons sequence, the Cycle Crossover is applied and for angles, the arithmetic crossover is appropriate. The whole crossover procedure is as follows:

Supposed 2 individuals in population are

(1, 26),(4, 120),(6, 96),(7, 302),(8, 16),(5, 359),(2, 0),(3, 270);

(4, 6),(7, 263),(1, 148),(3, 72),(5, 98),(8, 323),(6, 54),(2, 18).

Firstly, separate polygons sequence and angles of the gene block into two parts. The first part would be operated by cycle crossover and the second is prepared for the arithmetic crossover.

A. To the polygons sequence part:

Step 1:Find the cycle referring to the corresponding serial number of parents: 1-4-7-3-2-6-1;

Step 2:Copy the serial numbers of the first parent which is

also in the cycle to the first child;

Step 3:Delete the serial numbers of the second parent which is also in the cycle;

Step 4:Fill the blanks in the first child with leaving serial numbers of the second parent. The first child is fulfilled;

Step 5:Exchange the first parent and the second one, the second child could be attained in the same way.

The process of Cycle Crossover is listed in Fig.3.

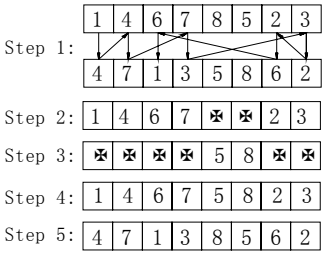


Fig.3. Principle of Cycle Crossover operator

B. To the angles Part:

The arithmetic crossover operator [9, 10] produces new individuals by linear combination two parents: Choose an appropriate crossover rate α, supposed parents in generation (t) are X_{A}^{t} and X_{B}^{t}, then the child should be:

$$X_{A}^{t+1} = \alpha X_{B}^{t} + (1-\alpha) X_{A}^{t},$$

$$X_{B}^{t+1} = \alpha X_{A}^{t} + (1-\alpha) X_{B}^{t}.$$

So to the angles part mentioned before:

$$\begin{bmatrix} 26 & 120 & 96 & 302 & 16 & 359 & 0 & 270 \\ 6 & 263 & 148 & 72 & 98 & 323 & 54 & 18 \end{bmatrix}$$

Choose crossover rate α=0.8 and corresponding child should be:

$$\begin{bmatrix} 10 & 234.4 & 137.6 & 118 & 81.6 & 330.2 & 43.2 & 68.4 \\ 22 & 148.6 & 106.4 & 256 & 32.4 & 351.8 & 10.8 & 219.6 \end{bmatrix}$$

3.6 Mutation operator:

A. To the polygons sequence Part: Two-point exchange mutation is available. To any polygons sequence, exchange two polygons position in it randomly and attain the new individual.

B. To the angles Part: Random mutation is available. Replace the angle of polygons with the random value possible and attain the new individual.

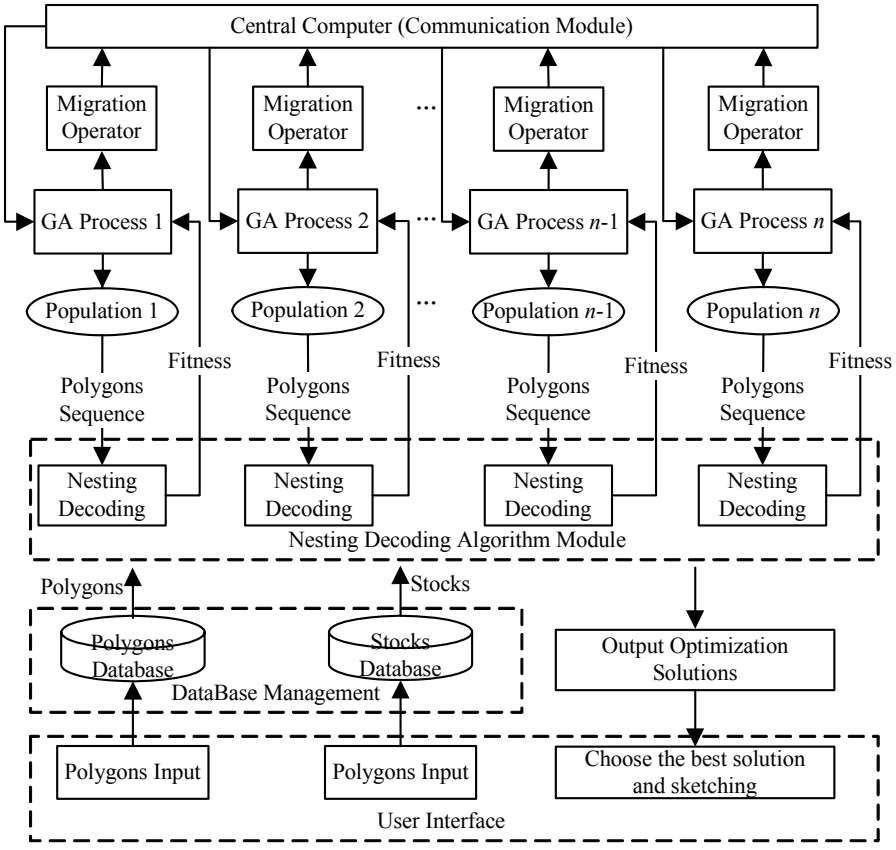


Fig.4. Structure of nesting system based on DPGA

4. THE NESTING DECODING ALGORITHM

The nesting decoding algorithm is particular rules set which could translates angles and sequence of polygons into practical arrangement in stocks. The bottom-left strategy is introduced detailedly in [5] is the most frequently used decoding algorithm in cutting stock problem. The bottom-left strategy sets the bottom-left corner of stock s as the start points. When a polygon is nested in, the start point would update to the polygon's top-right vertex; if the polygon is beyond stock's top-border, it would turn to the next column; and if beyond the stock's right-border, it would change to the next stock to

repeat the process until the last polygon is over. The flow of the bottom-left decoding algorithm is as following:

Step 1:Express all the stocks as $St_1, St_2, \cdots, St_n$ and all the irregular polygons as $G_1, G_2, \cdots G_n$;

Step 2:Set the bottom-left corner of stocks as the start points. Supposed the start point of $St_1, St_2, \cdots, St_n$ is $S_1, S_2, \cdots, S_n$, and the bottom-left vertex of polygon G_i is B_i, the top-right vertex of polygon G_i is T_i;

Step 3: Initialize polygons serials i=1;

Step 4: $i=i+1$;

Step 5: Initialize stock serials j=1;

Step 6: $j=j+1$;

Step 7: To polygon G_i, moving G_i according B_i to S_1 and fit G_i to the right position by the rule of never intersecting with other polygons before;

Step 8: If the current stock is full ,then $j=j+1$, go to Step 6 for another stock;

Step 9:If $X_{B_i} > X_{S_1}$,then $X_{S_1} = X_{B_i}$ and go to Step 10, else go to Step 11;

Step 10:If $Y_{B_i} > Y_{S_1}$, if yes, then $Y_{S_1} = Y_{B_i}$ .the start point has updated.

Step 11:If G_i is the last polygon, go to Step 12, else go to Step 4 for the next polygon.

Step 12:The Bottom-left nesting decoding is completed, out put nesting results.

4.2 The implement of the nesting system

The flow chart of the system is as Fig.4.

The system is developed by Visual Studio.Net and the genetic algorithm function is implemented by the help of Genetic Algorithm Optimization Toolbox (GAOT) [12] issued by North Carolina State University.

	Parts Number	*Time Elapsed (Approximately)*	*Time Reduced*
GA	20	24 min	
	50	42 min	
DPGA	20	18 min	25%
	50	27 min	36%

Table 1. Nesting by GA and DPGA

The nesting experiment is taken in a 4 computers distributed system, choosing population size as 40, crossover rate as 0.8, genetic generation as 200 and polygon number as 20 and 50.The comparison of traditional GA and DPGA is as Table 1: DPGA finishes nesting within 25%-36% time reduced of traditional GA and gets nearly fitness result. It proves the nesting system based on DPGA can improve the calculating speed. But it is obvious that speedup does hardly differ and fail to come close to the amount of processors being involved in the distributed system. Though DPGA can speed up calculating than traditional GA, linear speedup cannot be expected when calculating them in the way mentioned above anyway.

5. CONCLUSIONS

The paper presents a nesting system based on distributed genetic algorithm for 2-dimensitional polygons arts to solve the cutting stock problem in manufacturing. It mainly expounds the following scopes: Firstly, it discussed the application of traditional GA and distributed PGA; designed an appropriate distributed model fitting for the cutting stock problem solving. And then it describes the DPGA characteristic features in detail. At last, a nesting system based on DPGA is built up and it is proved to be efficient.

REFERENCES

[1] Al-Assaf, Y, “Human strategies based allocation of two-dimensional irregular shapes”,in J*ournal of Intelligent & Fuzzy Systems*,Vol.14(4),2003, pp.181~190.

[2] Chen, J.C, E.C.Han, “Research on the system of computer-aid cutting-stock”,in *Journal of South China University of Technology (Natural Science)*,Vol.29 (5), 2001, pp.42~44.

[3] Faina, L, “An application of simulated annealing to the cutting stock problem”,in *European Journal of Operational Research*,Vol.14 (3),1999,pp.542~556.

[4] Jiang, J.Q., X.L. Xing, et al, “A hybrid algorithm based on PSO and genetic operation and its applications for cutting stock problem”,in *Proceedings of the 2004 International Conference on Machine Learning and Cybernetics*,Vols.1-7.2004,pp.2198~2201.

[5] Edmund, B., H.Robert, et al, “A New Bottom-Left-Fill Heuristic Algorithm for the Two-Dimensional Irregular Packing Problem”,in *Operations Research*,Vol.54 (3), 2006,pp.587~596.

[6] A. Miguel Gomes, José F. Oliveira, “A 2-exchange heuristic for nesting problems”,in *European Journal of Operational Research*,Vol.141,Issue 2.1, Sep 2002, pp. 359~370.

[7] Bean, J. C., “A multiple-choice genetic algorithm for a nonlinear cutting stock problem”,in *Computing Science & Engineering* ,Vol.2 (2), 2000, pp.80~83.

[8] Fred F. Easton, “Nashat Mansour. A distributed genetic algorithm for deterministic and stochastic labor scheduling problems”,in *European Journal of Operational Research*,Vol.118,1999,pp.505~523.

[9] Erick Cant, David E. Goldberg, “Efficient parallel genetic algorithms: theory and practice”,in *Comput. Methods Appl. Mech. Engrg*,Vol.186,2000,pp.221~238.

[10] Zdeněk Konfŕst, “Parallel Genetic Algorithms: Advances, Computing Trends”,in *Proceedings of the 18th International Parallel and Distributed Processing Symposium*, 2004.

[11] Mitsuo Gen, Ruiwei Cheng, *Genetic Algorithms and Engineering Design*, New York: John Wiley & Sons, Inc. 1997.

[12] http://www.ise.ncsu.edu/mirage/GAToolBox/gaot/.

Wei Yang is currently a doctoral candidate in School of Power and Mechanical Engineering, Wuhan University. His research interests are Modern Design Methodology and CAD/CAM/CAE, etc.

Qingming Wu is currently a Full Professor and doctoral graduate supervisor in School of Power and Mechanical Engineering, Wuhan University. He has published over 10 Journal papers. His research interests are Modern Design Methodology and CAD/CAE/CAM, etc.

Shooting Algorithm of Soccer Robot Based on Bi-arc

Zaixin Liu, Weibing Zhu, Jinge Wang
Research Institute for Robot of Xihua University , Chengdu ,610039, China
E-mail: zhanxinliu@tom.com

ABSTRACT

To improve the rate of soccer robot shooting a goal, by analyzing shortcoming of basic shooting algorithm。Bi-arcs are used to solve the shooting problem of collision avoidance and holding appropriate position because they meet two end-point and two end-tangent conditions, namely the initial and terminal positions and tangents of mobile robots. The method presented here is simple，effective and computationally undemanding and it has no restraints on the initial conditions of soccer robot.

Keywords: Soccer Robot, Shoot, Bi-arc, Moving Path

1. INTRODUCTION

In the process of the soccer robot's goal-shooting, the frequently used basic algorithm[1] has the following procedures: (1) to calculate the shooting point of the robot; (2) to calculate the movement of the robot from the current position to the shooting point; (3) to adjust the angle of the robot so as to it keep the same attitude with the goal; (4) the goal shooting of the robot. Because the inertance is not taking into consideration, the trolley may run out of line with the goal point when it is adjusting its angle. Furthermore, when the trolley reaches the goal point。

It would take the factor of accuracy into consideration in adjusting angles. So it would have to slow down. Hence, the robot would go through the two processes of speeding-up and slowing-down when it moves from point of point. This undoubtedly has increased the time of shooting goal. And it has not calculate the factor of the blocking of other robots, which may delay the goal shooting attempts.

In the planning of the soccer robot's moving routes, the routes need to satisfy the soccer robot's initial position and its moving direction, its goal direction and its moving direction. We connect the sectionalized arc curves into bi-arcs, which bears the character of satisfying any random terminal points and its slope rate requirement[2], to solve the calculation of how to keep the best shooting position when the robot's encountering hindrances at its goal point in its shooting posture.

The routes planning strategy offered by the paper can be summarized as follows: given two terminal points and its tangent line, seek a sectionalized arc curve, make it satisfy the following conditions, 1) the curve must pass the two terminal points; 2) the curve must be tangent with the two tangent lines at the terminal points respectively; 3) the two arcs are connected by its continuity[3].

2. BI-ARC ALGORITHM

2.1 Bi-Arc Principle

Most of the function expressions of bi-arc curve are based on certain frame of axes, through the geometrical relationship, the radius was calculated out. Thought this algorithm is faultless in itself, but it can not be applied in the parameterized curve. So we proposed an expression which is based on vector computing and which is independent the frame of axes.

Write down the bi-arc as $\{P_s, T_s, P_e, T_e\}$, P_s and P_e the initial and goal point respectively. T_s is the unite tangent line of the current position, T_e expresses the straight tangent line which connect the ball P_e and the center point of goal O, that is $|T_s| = |T_e| = 1$. 1 and 2 represents current position of the enemy robots or the barrier. d_1、d_2 express the distance between 1 and 2 and the trolley's starting point P_s and its end point P_e

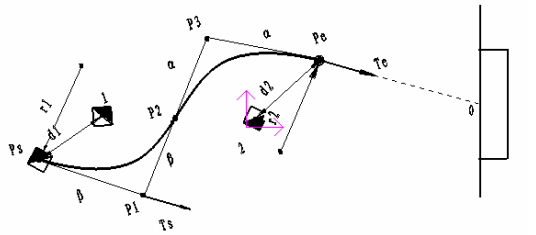


Fig.1. Bi- arc principle

According to the starting and ending point condition of fig.1, as long as the value of P_1、P_2 and P_3 are defined, the bi-arc could be determined. Since the unit tangent line is supposed as the terminal tangent line, hence

$$P_1 = P_s + \beta T_s \quad (1)$$

$$P_3 = P_e - \alpha T_e \quad (2)$$

$$\frac{P_3 - P_2}{\alpha} = \frac{P_2 - P_1}{\beta} \quad (3)$$

And

$$(P_1 - P_2)(P_1 - P_2) = \beta^2 \quad (4)$$

$$(P_2 - P_3)(P_2 - P_3) = \alpha^2 \quad (5)$$

from (3) $$P_2 = \frac{\beta P_3 + \alpha P_1}{\alpha + \beta} \quad (6)$$

put (6) into (4)、(5) the following:

$$P_1 - P_2 = \frac{\beta (P_1 - P_3)}{\alpha + \beta} = \frac{\beta (D + \beta T_s + \alpha T_e)}{\alpha + \beta} \quad (7)$$

$$P_2 - P_3 = \frac{\alpha (P_1 - P_3)}{\alpha + \beta} = \frac{\alpha (D + \beta T_s + \alpha T_e)}{\alpha + \beta} \quad (8)$$

Another condition: $D = P_s - P_e$

With this result we calculate by dots to (4), (5), after the simplifying process, we could have the following equation

$$D^2 + 2D(\beta T_s + \alpha T_e) + 2\alpha\beta (T_s T_e - 1) = 0 \quad (9)$$

In this equation, the unknown quantities are the constants α、β, according to the requirement of the arc radius r_1 and r_2, they could be uniquely determined. r_1 and r_2 could be determined by distance between the current position P_s and goal position P_e and the enemy robots position 1 and 2.

$r_1 = d_1 + 2l$; l (the length of the side) (10)
$r_2 = d_2 + 2l$

Through the solution of the equation, the value of α、β could be determined, then through the expression of P_1、P_2 and P_3, we could determine the positions of the 3 control points. Usually two arcs could satisfy all the routes planning, only under special circumstances, 4 arcs are required. The merits of the above mentioned approach has the advantage of easily identify and locate the bi-arc under the following special circumstance

$T_s T_e = \langle 1,-1 \rangle$; $D(\beta T_s + \alpha T_e) = 0$.

In the equations, the former one expresses that they goal direction parallel with the starting direction. (Or they are opposite to each other, that are parallel, but on different direction). The latter expresses the vertical relation between the terminal vector and the terminal line. Under these two circumstances, the bi-arc could be determined with the solution of the above quadratic equation.

2.2 Static Route Planning

Considering the errors brought about by inertance and the probability in shooting goals, we generally locate the midpoint of the goal as the goal point. In live competition, however, the goalkeeper of the opposite side would occupy the midpoint of the goal. Furthermore, there would be two players assisting the defense in the bigger penalty area (see 3 and4 in the figure). Under this circumstance, if the shooting still aims at the O point or OB zone, the goal would easily be blocked by play 3 and play 4[4]. The best shooting point would be in the zone OB' now. Taking into consideration of error and probability, we locate the midpoint O' of zone OB' as the best shooting point. So when the initial position of the robot and the position of the ball are given, the moving direction of the robots and its moving direction when reaching the shooting position are as illustrated in Fig. 2.

According to the bi-arc principles mentioned above, regarding the route planning of the robot, as long as we can locate the points P_{s1} and P_{e1}, we could get the value of all the control points P_1、P_2、P_3、P_4、P_5 and P_6 through the two control point equation of bi-arc. And the value of point P_{s1} and point P_{e1} could be figure out through 4 section arc, which is a special variant of bi-arc, and its geometrical relation, the easily realized continuous and smooth bi-arc routes as illustrated in the following figures.

2.3 Dynamic Trace Routes Planning

In the movement of the trolley, the current position of the robot and the position of the goal point are always changing. And the positions of the enemy robots are also changing. See Fig.3,

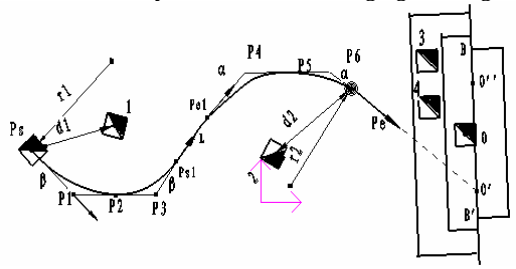


Fig.2. Static routes planning

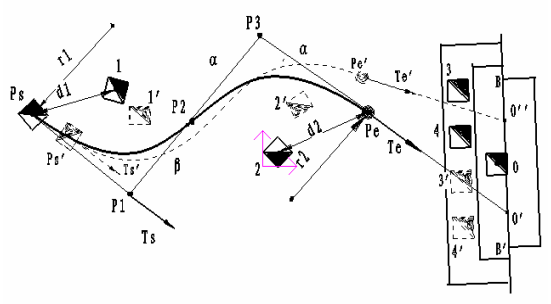


Fig.3. Dynamic trace routes planning

when robot moves from point P_s at time t_i to point P_s' at time t_{i+1}, and the enemy robot 1 and 2 move from the illustrated position to $1'$ and $2'$, assisting players 3 and 4 move to position 3' and 4'. The best shooting position now shift from zone OB' to zone OB, the goal point shift from point O' to O''. Due to the change in robot's current position and the relative position of the goal point and the change in position and the block's position, so the moving trace of the robots at time t_{i+1} are no longer the former bi-arc $\{P_s, T_s, P_e, T_e\}$, but the new bi-arc $\{P_s', T_s', P_e', T_e'\}$ (the broken line in the figure). Now the moving trace of the trolley after a certain time ($\Delta t = t_{i+1} - t_i$) needs to be planned again. The final moving trace of the robot is on longer the regular bi-arc, but a smooth and continuous irregular curve.

3. CONCLUSIONS

The paper has proposed a new algorithm on soccer robot's goal shooting through the approach of bi-arc, that is, to solve the calculation of shooting goal of moving robots through bi-arc. Figure 4 is the program flow diagram of route planning.

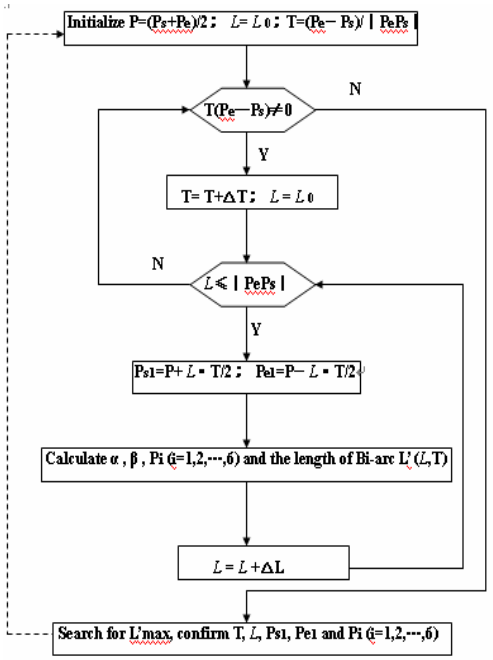


Fig.4. Program flow diagram

The static planning of robot's reaching target points (that is, the position of the ball, its moving direction is the line drawn between the ball and midpoint of the goal) at a given time are

illustrated by actual line. The broken line indicates the re-planning of the routes after certain duration according to the change of situation on the field. Figure 5 give a emulation experiment example on route planning. We could find that the moving traces of the robots are no longer the regular bi-arc, but a smooth and irregular curve. This method is simple and effective. The initial condition of robots is not restrictive, can function with small amount of calculation. It could be applied into searching, exploration, astronomies and aeronautics.

Fig.5. Result of bi-arc shooting experiment

REFERENCES

[1] HAN Xue-dong, HONG Bing-rong, MENG Wei. "Shooting algorithm in robot soccer." *Journal of harbin institute of technology*,2003, 35(9):1064-1065

[2] Moreton D N, Parkinson D B. "The application of bi-arc technique in CNC athining". *Computer-Aided Engineering Design Journal*, 1991,8:54-60

[3] Meek D S, Walton D J. "Approximation of discrete data by G'arc splines."*Computer-Aided Design*, 1992, 24(6): 301-306

[4] HAO Zong—bo, "HONG Bing-rong, Shooting action of simulation robot soccer." *Journal of harbin institute of technology*,, 2003, 35(9):1102-1103

Zaixin Liu: Lecturer, Master. He graduated from Hubei Industry University in 2001. In 2004, he got the master degree in Xihua University. He has been teaching since 2004 in Xihua University. His research focus on the intellectual robot technology and draft system of mechanics. Till now, has been taken part in many research programmers of Sichuan province and the Industry Ministry. He has published more than ten papers in different international and civil journals.

The Block Parallel Computation of Matrix Tensor Production *

Guolv Tan
Department of Mathematic & Computer, ShangRao Normal College
ShangRao, Jiangxi 334001, China
Email: TAN-GL@163.com

ABSTRACT

In matrix computation, the computation of matrix tensor product is an important problem. Compared with its multiplication, the computing amount of tensor product is huger. Based on analyzing its mathematical properties, a result is proved that two matrices tensor operation can be exchanged in the sense of permuted similar, and the convenient method for constructing the permutation matrix is given. Furthermore, a conclusion is obtained that tensor product of block matrixes can be block calculated in the sense of permuted similar. Based on these, the parallel computing models of matrix tensor product are proposed. From an example, the thought and process of the algorithm are showed.

Keywords: Block Matrix, Tensor Product, Permuted Similar, Parallel Computing, Algorithm Complexity

1. INTRODUCTION

In domains such as engineering design and numerical algebra, many computation problems can finally be conclusion to the matrix computation problem, which needs to use parallel machine system to carry on massively parallel computation. Because the computational amount is huge, therefore how effectively carries on these matrix computation is extremely important, and it causes many scholars research interest, emerge many research results, in which there are famous Cannon algorithm and Fox algorithm. In paper [1], the author proposes a matrix-multiplication algorithm suited to the distributed computer environment on PVM; In paper [2], the author design a new parallel algorithm for matrix multiplication by Gramian of Toeplitz-block matrix; Literature [3] has realized the Cannon algorithm on the cluster of workstations; Literature [4] presented a new parallel algorithm for matrix multiplication based on diagonal partition strategy, and so on. In paper [5], the author proposed a kind data Encryption scheme by matrix tensor theories, in which he uses some low-scale matrices to construct the structure complex high-scale matrix through tensor production. According to mathematics definition, compared with its multiplication, the computational amount of matrices tensor production is huger. In order to effectively carrying on the parallel computation of matrix tensor production, this paper studies block operation properties of the matrices tensor production and discuss its parallel computation problem.

2. THE BLOCK OPERATION PROPERTIES OF MATRICES TENSOR PRODUCTION

Let us denote all $n\times m$ matrices by $M_{n,m}$ and the series set $\Gamma(n_1,n_2,\cdots,n_m)=\{\alpha\mid\alpha=(\alpha(1),\cdots,\alpha(m);1\le\alpha(i)\le n_i, i=1,\cdots,m\}$. $\Gamma(n_1,n_2,\cdots,n_m)$ is simply denoted as $\Gamma_{m,n}$ when $n_1=\cdots=n_m=n$.

For $A_p=(a_{ij}^p)\in M_{s_p,t_p}$, $p=1,2,\cdots,m$, theirs tensor product define as below

$$A_1\otimes A_2\otimes\cdots\otimes A_m=(a_{\alpha\beta})_{s\times t} \quad (1)$$

where $s=\prod_{p=1}^{m}s_p$, $t=\prod_{p=1}^{m}t_p$, $a_{\alpha\beta}=\prod_{p=1}^{m}a^{(p)}_{\alpha(p)\beta(p)}$, $\alpha\in\Gamma(s_1,s_2,\cdots,s_m)$ and $\beta\in\Gamma(t_1,t_2,\cdots,t_m)$. We simply denote the $A_1\otimes A_2\otimes\cdots\otimes A_m$ as $\bigotimes_{p=1}^{m}A_p$.

The matrix $\bigotimes_{p=1}^{m}A_p$ is a large matrix with $\prod_{p=1}^{m}s_p$ rows and with $\prod_{p=1}^{m}t_p$ columns and its element of α row β column is $\prod_{p=1}^{m}a^{(p)}_{\alpha(p)\beta(p)}$, here α,β are ordered by dictionary series.

A square matrix which every row and every column had only one component equal to 1 and other components equal to 0 is called a permutation matrix.

From (1), we can easily certify the below conclusion.

Lemma 1 Let $A=(a_{ij})\in M_{n,m}$ and B be a matrix. Then

$$A\otimes B=\begin{pmatrix}a_{11}B & a_{12}B & \cdots & a_{1m}B\\ a_{21}B & a_{22}B & \cdots & a_{2m}B\\ \vdots & \vdots & \vdots & \vdots\\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B\end{pmatrix}.$$

Theorem 1 Let $A=(a_{ij})\in M_{n,m}$ and $B=(b_{ij})\in M_{s,t}$. Then there exist a $ns\times ns$ permutation matrix P_1 and $mt\times mt$ permutation matrix P_2, such that

$$B\otimes A=P_1(A\otimes B)P_2.$$

Proof. $A\otimes B$ is a $ns\times mt$ matrix. We construct a permutation matrix $P_{m,t}$ as below:

$P_{m,t}$ is a $mt\times mt$ matrix, and its rows is equal to the element numbers of the set $\Gamma(t,m)$ (or set $\Gamma(m,t)$). Let $\alpha=(\alpha(1),\alpha(2))\in\Gamma(t,m)$, then $\alpha'=(\alpha(2),\alpha(1))\in\Gamma(m,t)$. Let ε_i denoted a column-vector with its ith component equal to 1 and with all other components equal to 0. Then the $(\alpha(1)-1)\times m+\alpha(2)$ -th column-vector of $P_{m,t}$ is equal to $\varepsilon_{(\alpha(2)-1)\times t+\alpha(1)}$.

Now we can directly verify that

$$B\otimes A=P_{n,s}^{-1}(A\otimes B)P_{m,t}=P_{n,s}^{'}(A\otimes B)P_{m,t}.$$

Remark: The matrix $P_{n,s}$ in theorem 1 has not any relation with the concrete content of matrix A and B, but only with n (the rows of matrix A) and s (the rows of matrix B). Moreover, it can be specifically write out only by n and s. The similar result is hold for the matrix $P_{m,t}$. For example, let $\alpha=(1,2)\in\Gamma(5,4)$, then

$\alpha'=(2,1)\in\Gamma(4,5)$, $(\alpha(1)-1)\times 4+\alpha(2)=2$, $(\alpha(2)-1)\times 5+\alpha(1)=6$

Hence the 2-th column-vector of $P_{4,5}$ is ε_6. Therefore, we obtained that $P_{4,5}$ =

* The project was supported by the Natural Science Foundation of Jiangxi(0411030).

$\{\varepsilon_1,\varepsilon_6,\varepsilon_{11},\varepsilon_{16},\varepsilon_2,\varepsilon_7,\varepsilon_{12},\varepsilon_{17},\varepsilon_3,\varepsilon_8,\varepsilon_{13},\varepsilon_{18},\varepsilon_4,\varepsilon_9,\varepsilon_{14},\varepsilon_{19},\varepsilon_5,\varepsilon_{10},\varepsilon_{15},\varepsilon_{20}\}$

$=\{1000000000000000000;\ 0000010000000000000;$
$0000000001000000000;\ 0000000000000010000;$
$0100000000000000000;\ 0000001000000000000;$
$0000000000100000000;\ 0000000000000001000;$
$0010000000000000000;\ 0000000100000000000;$
$0000000000010000000;\ 0000000000000000100;$
$0001000000000000000;\ 0000000010000000000;$
$0000000000001000000;\ 0000000000000000010;$
$0000100000000000000;\ 0000000001000000000;$
$0000000000000100000;\ 0000000000000000001\}$.

Additional, we can easily certify that $P_{n,s}^{-1}=P_{n,s}^{'}=P_{s,n}$.

Corollary 1 Let n,s,m,t be positive integers. Then there exist permutation matrix $P_{n,s}$ and $P_{m,t}$, such that

$B\otimes A=P_{n,s}^{'}(A\otimes B)P_{m,t}$ for $\forall A\in M_{n,m}$ and $\forall B\in M_{s,t}$.

Based on Theorem 1, the matrix A is said permuted similar to matrix B, if there exist permutation matrix P and Q, such that $B=PAQ$.

Obviously, the combination law is hold for matrix tensor production, e.g., $\overset{m}{\underset{i=1}{\otimes}}A_i=(A_1\otimes\cdots\otimes A_s)\otimes(A_{s+1}\otimes\cdots\otimes A_m)$, where $0\le s\le m$.

Theorem 2 Let $A=(A_{ij})_{n\times m}$ be a block matrix and B be a matrix. Then the follow equation is hold.

$$A\otimes B=\begin{pmatrix}A_{11}\otimes B & \cdots & A_{1m}\otimes B\\ \cdots & \cdots & \cdots\\ A_{n1}\otimes B & \cdots & A_{nm}\otimes B\end{pmatrix}$$

Proof. According to Lemma 1, it can be directly verified.

Theorem 3 Let $A=(A_{ij})_{n\times m}$ and $B=(B_{pq})_{s\times t}$ be block matrices, where $A_{ij}\in M_{n_i,m_j}$ for $i=1,2,\cdots,n;\ j=1,2,\cdots,m$ and $B_{pq}\in M_{s_p,t_q}$ for $p=1,2,\cdots,s;q=1,2,\cdots,t$. Then $A\otimes B$ is permuted similar to the follow matrix

$$\begin{pmatrix}A_{11}\otimes B_{11} & \cdots & A_{11}\otimes B_{1t} & \cdots\cdots & A_{1m}\otimes B_{11} & \cdots & A_{1m}\otimes B_{1t}\\ \cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & \cdots\\ A_{11}\otimes B_{s1} & \cdots & A_{11}\otimes B_{st} & \cdots\cdots & A_{1m}\otimes B_{s1} & \cdots & A_{1m}\otimes B_{st}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ A_{n1}\otimes B_{11} & \cdots & A_{n1}\otimes B_{1t} & \cdots\cdots & A_{nm}\otimes B_{11} & \cdots & A_{nm}\otimes B_{1t}\\ \cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & \cdots\\ A_{n1}\otimes B_{s1} & \cdots & A_{n1}\otimes B_{st} & \cdots\cdots & A_{nm}\otimes B_{s1} & \cdots & A_{nm}\otimes B_{st}\end{pmatrix}. \quad (2)$$

Proof. Form theorem 2, we have

$$A\otimes B=\begin{pmatrix}A_{11}\otimes B & \cdots & A_{1m}\otimes B\\ \cdots & \cdots & \cdots\\ A_{n1}\otimes B & \cdots & A_{nm}\otimes B\end{pmatrix}.$$

According to corollary 1 of theorem 1, for each A_{ij}, there exist permutation matrix $P_{n_i,h}$ and $P_{m_j,l}$, where $h=\prod_{k=1}^{s}s_k, l=\prod_{k=1}^{t}t_k$, such that

$P_{n_i,h}^{'}(A_{ij}\otimes B)P_{m_j,l}=B\otimes A_{ij}$ for $i=1,2,\cdots,n;\ j=1,2,\cdots,m$.

Let the permutation matrix $P_1=diag\{P_{n_1,h},\cdots,P_{n_n,h}\}$ and the permutation matrix $P_2=diag\{P_{m_1,l},\cdots,P_{m_m,l}\}$. Then

$$P_1^{'}(A\otimes B)P_2=\begin{pmatrix}P_{n_1h}^{'}(A_{11}\otimes B)P_{m_1,l} & \cdots & P_{n_1,h}^{'}(A_{1m}\otimes B)P_{m_m,l}\\ \cdots & \cdots & \cdots\\ P_{n_n,h}^{'}(A_{n1}\otimes B)P_{m_1,l} & \cdots & P_{n_n,h}^{'}(A_{nm}\otimes B)P_{m_m,l}\end{pmatrix}$$

$$=\begin{pmatrix}B\otimes A_{11} & \cdots & B\otimes A_{1m}\\ \cdots & \cdots & \cdots\\ B\otimes A_{n1} & \cdots & B\otimes A_{nm}\end{pmatrix}.$$

From theorem 2, we have

$$B\otimes A_{ij}=\begin{pmatrix}B_{11}\otimes A_{ij} & \cdots & B_{1t}\otimes A_{ij}\\ \cdots & \cdots & \cdots\\ B_{s1}\otimes A_{ij} & \cdots & B_{st}\otimes A_{ij}\end{pmatrix} \quad (3)$$

From theorem 1 again, there exist permutation matrix P_{s_p,n_i} and P_{t_q,m_j}, such that

$$P_{s_p,n}^{'}(B_{pq}\otimes A_{ij})P_{t_q,m_j}=A_{ij}\otimes B_{pq}$$

for $i=1,2,\cdots,n;\ j=1,2,\cdots,m$ and $p=1,2,\cdots,s;q=1,2,\cdots,t$.

Let $P_3=diag\{P_{s_1,n_1},\cdots,P_{s_s,n_1},\cdots\cdots,P_{s_1,n_n},\cdots,P_{s_s,n_n}\}$ and $P_4=diag\{P_{t_1,m_1},\cdots,P_{t_t,m_1},\cdots\cdots,P_{t_1,m_m},\cdots,P_{t_t,m_m}\}$. Now, the formula (2) is equal to $P_3^{'}P_1^{'}(A\otimes B)P_2P_4$.

3. PARALLEL COMPUTATION FOR MATRIX TENSOR PRODUCTION

Let $A_1,A_2,\cdots,A_m\in M_{n,n}$ be invertible matrices. We knew that $(\overset{m}{\underset{i=1}{\otimes}}A_i)^{-1}=\overset{m}{\underset{i=1}{\otimes}}A_i^{-1}$. But for the large $n^m\times n^m$ matrix $\overset{m}{\underset{i=1}{\otimes}}A_i$, it is very difficult to calculate its inverse matrix when don't knew it was the m-tuples tensor production of $n\times n$ matrix.

According to paper [5], it has a strong advantage for construct the encryption matrix by using matrix tensor product.

According to equation (1), it should make $(m-1)n^{2m}$-times multiplication to calculate the m-tuples tensor product of $n\times n$ matrix, and should need n^{2m}-times multiplication by using the combination law of matrix tensor product. So, the computational amount is every huger when n and (or) m be relatively big. In the following, we discuss the parallel computing problem of the matrix tensor production by using the property of block tensor production operation.

Algorithm 3-1 Assume $A_1=(a_{ij})_{n\times n}$ and A_2 be $n\times n$ matrix. There are $n\times n$ processors with Mesh-Connected and receptivity denoted as P_{ij}. According to lemma 1, we can compute $A_1\otimes A_2$ by following method.

Put the element of A_1 separately into the processors (a_{ij} on P_{ij}). Put A_2 into every processor. Then $a_{ij}A_2$ is computed in processor P_{ij} for parallel all $i,j=0,1,\cdots,n-1$. Finely, we obtained the computing result of $A_1\otimes A_2$ by recovering the results of all processors.

In the following, we analyzed the algorithm complexity. In order to facilitate the description, here omits the recovery process. And the algorithm complexity is only measured by the total times of multiplication.

The total times of multiplication is n^2 for computing $a_{ij}\otimes A_2$ in P_{ij}. Hence, the cost $c(n)=t(n)\cdot p(n)=n^4$, the accelerated-rate $S_p(n)=\frac{t_s(n)}{t_p(n)}=\frac{n^4}{n^2}=n^2$, the efficiency $E_p(n)=\frac{S_p(n)}{p(n)}=O(1)$. These indicators show that the parallel algorithm is optimal.

Algorithm 3-2 Suppose that $A=(A_{ij})_{n\times n}$ be a block matrix (where A_{ij} is a $m\times m$ matrix) and B be a $n\times n$ matrix. There are $n\times n$ processors with Mesh-Connected and receptivity denoted as P_{ij}. According to theorem 2, we can compute $A\otimes B$ by the following method.

Put A_{ij} into the processor P_{ij}. Put B into every processor. Then $A_{ij}\otimes B$ is computed in processor P_{ij} for parallel all $i,j=0,1,\cdots,n-1$. Finely, we obtain the computing result of $A\otimes B$ by recovering the results of all processors.

The total times of multiplication is m^2n^2 for computing $P_{ij}\otimes B$ in P_{ij}. Hence, the cost of the parallel computing is m^2n^4, the accelerated-rate $S_p(n)=m^2n^2$, the efficiency $E_p(n)=O(m^2)$.

Algorithm 3-3 Suppose that $A=(A_{ij})_{n\times n}$ ($i,j=0,1,\cdots,n-1$) and $B=(B_{pq})_{n\times n}$ ($p,q=0,1,\cdots,n-1$) be block matrices. There are $n\times n$ processors with Mesh-Connected and receptivity denoted as P_{ij}. According to theorem 3, in ordering to compute $A\otimes B$, we introduce $C_{ij}=(B_{pq}\otimes A_{ij})$ where C_{ij} is divided into $n\times n$ sub-blocks $B_{pq}\otimes A_{ij}$ ($p,q=0,1,\cdots,n-1$). Put A_{ij}, B_{ij} and C_{ij} into the local memory of processor P_{ij}, where C_{ij} is a zero matrix previously. Now we compute the tensor production of two sub matrices, where the sub matrices are storage in the local memory of processor P_{ij}. First, we set $p=i$ and $q=j$.

Step 1: computing $B_{pq}\otimes A_{ij}$ in processor P_{ij}, and storing the result into the (p,q)-th sub-block of C_{ij}.

Step 2: Set $q\leftarrow(q+1) \bmod n$, this making the sub-blocks of B cyclic shift toward left.

Step 3: If $q\neq j$ then goto *step 1*, else goto *step 4*.

Step 4: Set $p\leftarrow(p+1) \bmod n$.

Step 5: If $p\neq i$ then making the sub-blocks of B cyclic shift toward upward and goto *step 1*, otherwise goto *step 6*.

Step 6: Now we take the permuted replacement to C_{ij} as in theorem 3. Finally we obtained the computing result of $A\otimes B$ by recovering the results of all processors.

To conveniently estimate the computational complexity of algorithm 3-3, we assume that A_{ij} and B_{pq} are both $m\times m$ matrix and omit the communication time between processors and the times of reorganizing C_{ij}. There need n^2m^4 multiplication for computing $B_{pq}\otimes A_{ij}$ in processor P_{ij}. Hence, the cost $c(n)=t(n)\cdot p(n)=n^4m^4$, and the accelerated-rate $S_p(n)=\dfrac{(nm)^4}{n^2m^4}=n^2$.

For $i=1,2,\cdots,m$, let $A_i=(A_{pq}^{(i)})_{n\times n}$ be block matrices. According to theorem 3, $\overset{m}{\underset{i=1}{\otimes}}A_i$ is permuted similar to $\left(\overset{m}{\underset{i=1}{\otimes}}A^{(i)}_{\alpha(i)\beta(i)}\right)$, $\alpha,\beta\in\Gamma_{m,n}$. Thus, we can compute the tensor product $\overset{m}{\underset{i=1}{\otimes}}A_i$ by repeating call algorithm 3-3 and using the combination-law of matrix tensor product.

4. EXAPLE FOR ALGORITHM

Now, we cite an example for algorithm 3-3. To save space, we take a lower scale matrix, but it enough to exposited the algorithm thought and computing procedure.

Let

$$A=\begin{pmatrix}41&61&30\\55&72&53\\18&19&23\end{pmatrix}=\begin{pmatrix}A_{00}&A_{01}\\A_{10}&A_{11}\end{pmatrix},\ B=\begin{pmatrix}43&31&11&13\\21&7&47&17\\29&5&39&86\\27&73&87&91\end{pmatrix}=\begin{pmatrix}B_{00}&B_{01}\\B_{10}&B_{11}\end{pmatrix},$$

where $A_{00}=\begin{pmatrix}41&61\\55&72\end{pmatrix}$ and $B_{00},B_{01},B_{10},B_{11}$ are 2×2 matrices. In below,we examine the computational process in processor P_{00}.

First, $B_{00}\otimes A_{00}$ is computed on P_{00} and the result is storage in the $(0,0)$-th block of C_{00}. Then take the sub-blocks of B cyclic shift toward left. Thus B_{01} is moved to P_{00}. $B_{01}\otimes A_{00}$ is computed on P_{00} and the result is storage in the $(0,1)$-th block of C_{00}. Take the sub-blocks of B cyclic shift toward left again and it makes B resumed. Then take the sub-blocks of B cyclic shift toward upward and thus B_{10} is moved on P_{00}. $B_{10}\otimes A_{00}$ is computed on P_{00} and the result is storage in the $(1,0)$-th block of C_{00}. Take the sub-blocks of B cyclic shift toward left again and B_{11} is moved to P_{00}. $B_{11}\otimes A_{00}$ is computed on P_{00} and the result is storage in the $(1,1)$-th block of C_{00}. Finally, C_{00} is formed and it is equal to the following matrix.

(1763,2623,1271,1891,451,671,533,793;
2365,3096,1705,2232,605,792,715,936;
861,1281,287, 427,1927,2867,697,1037;
1155,1512,385,504,2585,3384,935,1224;
1189,1769,205,305,1599,2379,3526,5246;
1595,2088,275,360,2145,2808,4730,6192;
1107,1647,2993,4453,3567,5307,3731,5551;
1485,1944,4015,5256,4785,6264,5005,6552).

Next, we adjust C_{00}. According to theorem 3, let $P'_{2,4}=(\varepsilon_1,\varepsilon_3,\varepsilon_5,\varepsilon_7,\varepsilon_2,\varepsilon_4,\varepsilon_6,\varepsilon_8)$. So, we rearrange the columns of C_{00} by order of 1,3,5,7,2,4,6,8 and then rearrange the rows by order of 1,3,5,7,2,4,6,8. Now, we obtained that $P_{2,4}C_{00}P'_{2,4}=$

(1763,1271,451,533,2623,1891,671,793;
861,287,1927,697,1281,427,2867,1037;
1189,205,1599, 3526,1769,305,2379,5246;
1107,2993,3567,3731,1647,4453,5307,5551;
2365,1705,605,715,3096, 2232,792,936;
1155,385,2585,935,1512,504,3384,1224;
1595,275,2145,4730,2088,360,2808,6192;
1485,4015,4785,5005,1944,5256,6264,6552)

The case of other processors is similar. Finally, $A\otimes B$ is computed and it is equal to the following matrix.

(1763,1271,0451,0533,2623,1891,0671,0793,1290,0930,0330,0390
0861,0287,1927,0697,1281,0427,2867,1037,0630,0210,1410,0510
1189,0205,1599,3526,1769,0305,2379,5246,0870,0150,1170,2580
1107,2993,3567,3731,1647,4453,5307,5551,0810,2190,2610,2730
2365,1705,0605,0715,3096,2232,0792,0936,2279,1643,0583,0689
1155,0385,2585,0935,1512,0504,3384,1224,1113,0371,2491,0901
1595,0275,2145,4730,2088,0360,2808,6192,1537,0265,2067,4558
1485,4015,4785,5005,1944,5256,6264,6552,1431,3869,4611,4823
0774,0558,0198,0234,0817,0589,0209,0247,0989,0713,0253,0299
0378,0126,0846,0306,0399,0133,0893,0323,0483,0161,1081,0391
0522,0090,0702,1548,0551,0095,0741,1634,0667,0115,0897,1978
0486,1314,1566,1638,0513,1387,1653,1729,0621,1679,2001,2093)

5. CONCLUSIONS

By researching the relational mathematical property of block matrix tensor product, this paper discussed the block parallel computation problem of the matrix tensor product, and given the concrete computation models. The practice proved that this parallel algorithm can achieve a good effect in computing large-scale matrices tensor product.

REFERENCES

[1] Masamitsu Hattori, Nobuhiro Ito, Wei Chen, et al. "Parallel Matrix-Multiplication Algorithm for Distributed Parallel Computers[J]." *Systems and Computers in Japan*, 2005, 36(4):48-59

[2] Gabriel Oksa; Martin Becka; *Marian Vajtersic. Parallel algorithm for matrix multiplication by Gramian of Toeplitz-block matrix[C]*. IASTED International Conference on Applied Informatics, International Sympsosium on Parallel and Distributed Computing and Networks. Innsbruck, Austria. 2002:53-58

[3] LI Xiaozhou, LI Qinghua. "Implementation of Matrix Multiple Cannon Parallel Algorithm on Cluster of Workstations[J]." *Computer Engineering*, 2002,28(6): 102-103, 107(In Chinese)

[4] ZHANG Xuebo, LI Xiaomei. "A Parallel Algorithm for Matrix Multiplication Based on Diagonal Partition Strategy[J]." *Computer Engineering*, 2004,30(6):42-43 (In Chinese)

[5] TAN Guolv. "A Kind of Data Encryption Scheme Based on the Tensor Product of Matrices[J]." *COMPUTER SCIENCE*, 2002,29(8):119-120,125(In Chinese)

Guolv Tan (1957-) is a Professor and a head of Computer Science and Technology, Associate director of Mathematics & Computer Department, Shangrao normal college. He obtained his masters degree from Beijing Normal University. He is an instructor of computer software and theory. He has published over 30 Journal papers. His research interests are in parallel distributed processing and cryptography.

A Path Finding Algorithm of Mobile Robot for Bridging Special Obstacles

Qiaoyu Sun[1], Yinrong Pan[2]
[1]Department of Electronic Engineering, Huaihai Institute of Technology
Lianyungang, Jiangsu, China
[2]Department of Computer Science and Technology, East China Normal University
Shanghai, China
Email: qiaoyusun@163.com

ABSTRACT

This paper presents an algorithm, which is used to find a shortest path between two given nodes in a grid with sparse polygon obstacles. Some obstacles could be bridged. The algorithm executes the search using a "don't change direction" heuristic along the line towards the target node. The path has eight searching directions, which decided by the opposition of source and target nodes. According to the result of many contrastive on-the-fly experiments, the algorithm reduces the size of searching region. The path length is also shorter than that was found using traditional algorithm. It is an efficient algorithm.

Keywords: Shortest Path, Sparse Obstacle, Minimum Detour, Grid Graph

1. INTRODUCTION

The path programming technique is an important branch of the robot research. The path programming technique of robots is to find an optimum path between two nodes in the work plane according one or more rules (eg: minimum work cost, shortest path length or lest time etc.) which can avoid obstacles. Originally, Robot was born to replace person on doing some works, so it in fact is imitating the person's action. Person can decide quickly to avoiding or bridging the obstacle in real life, so robot should not avoid the obstacle simply. This paper gives an obstacle-avoiding path find algorithm which can bridge some obstacles in grids. It has eight directions to expand the path.

2. SEARCHING TECHNIQUE

This algorithm looks for a shortest path between two given nodes in R × R grid that has sparse obstacles (obstacle for occupying≤10%). Each node has eight expanding directions: up(*dir*=2);down(*dir*=-2); left(*dir*=-3); right(*dir*=3); right-up(*dir*=4); right-down(*dir*=5); left-up(*dir*=-5); left-down(*dir*=-4).
The position of source and target nodes is *S*(*Xs*, *Ys*), *T*(*Xt*, *Yt*).The length of shortest path between the two points is $\sqrt{2}$ min(| *Yt*-*Ys*|,| *Xt*-*Xs*|)+|| *Yt*-*Ys*|-| *Xt*-*Xs*|| while having no obstacle. It will increase when hitting obstacle. The differ is decided by the detour length when the path avoiding obstacles. So the path should decide its expanding direction on which has less detour length.

The algorithm executes the search using a "don't change direction" heuristic along the line towards the target node. The algorithm include primarily below several parts:

2.1 Original Searching Direction

The searching direction *dir* is decided according to the position of source node and target node:
If *Xt*>*Xs* and *Yt*=*Ys*: *Dir*=3; If *Xt*>*Xs* and *Yt*>*Ys*: *Dir*=4;
If *Xs*>*Xt* and *Yt*=*Ys*: *Dir*=－3; If *Xt*>*Xs* and *Yt*<*Ys*: *Dir*=－4;
If *Yt*>*Ys* and *Xs*=*Xt*: *Dir*=2; If *Yt*>*Ys* and *Xt*<*Xs*: *Dir*=－5;
If *Yt*<*Ys* and *Xs*=*Xt*: *Dir*=－*2*; If *Yt*<*Ys* and *Xt*>*Xs*: *Dir*=5.

As part of the printing process your document will be photographed. To ensure that this can be done with one camera setting for all papers and to ensure uniformity of appearance for the Proceedings, your paper should conform to the following specifications. If your paper deviates significantly from these specifications, the printer may not be able to include your paper in the Proceedings.

2.2 Operation of Hitting Obstacle

When the searching hit an obstacle, if the obstacle can be bridged, it will bridge the obstacle and go on with its original direction.

If the obstacle can't be bridged, search the coordinate of the obstacle's extreme firstly. Then, look for the direction of around the obstacle: the path which has shorter detour should be selected (if one of the obstacle's edge is adjacent to the border of grid, the path will go around the obstacle in the opposite direction) .

Some circumstance may appear while going round the obstacle:

(1) **Expand to the extreme of the obstacle B_1:**

In figure 1－(a) ,when the path expanded to the top extreme Y_h (X_b is the horizontal coordinate of nearer extreme, X_f is the horizontal coordinate of farther; Y_h is the vertical coordinate of top extreme, Y_l is the vertical coordinate of bottom extreme), its direction will be change to right and expand currently to X_f.Choose the expanding direction from eight original direction according to the oppsition of current node and target node and go on expanding until hit an other obstacle.

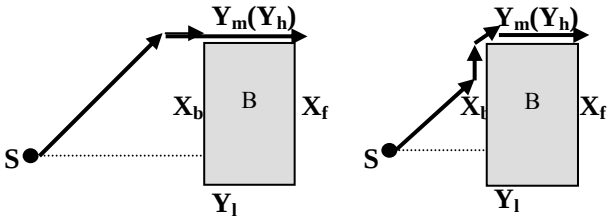


Fig.1. Operation of expanding to the extreme of obstacle

When the path has expanded to the extreme of obstacle B_1. The extreme is the nearest extreme X_b, but not the selected one, such as figure 1－(b).Change the current direction to up and expand to Y_m（Y_m is vertical coordinate of the selected extreme; X_m is horizontal coordinate of the selected extreme）.Then, change the direction to right and expand to X_f. Choose the

expanding direction according to the opsition of current node and target node and go on expanding until hit an obstacle.

(2) **Hit the obstacle B_2 in expanding.**

B_2 should be gone round first, such as figure 2.If the obstacle is to the right of path, the path will go back to Y_m'(the bottom extreme of B_2) and change the expanding direction same to the horizontal sub_direction of current direction. In the figure 2 the direction is right until expanding to X_f'. Go on expanding with the original direction (right-up).

If hit a new obstacle B_3, and it is to the top of path, the expanding direction will be changed same to the horizontal sub_direction of current direction. In the figure 2 the direction is right until expanding to X_f''. Go on expanding with the original direction (right-up) until hit X_f.

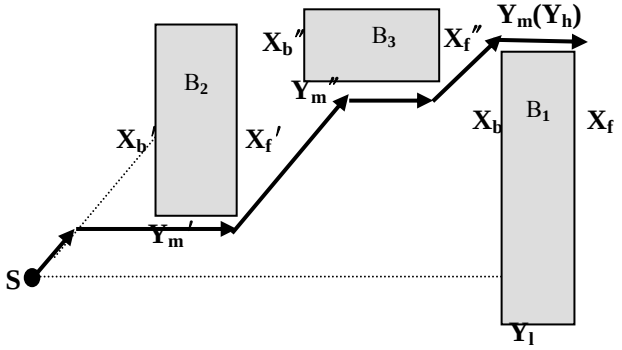


Fig.2. Operation if hit another obstacle while going round the obstacle

(3) **Hits the obstacle B_2 while going round the last extreme of B_1**

As figure 3, B_2 is adjacent to B_1， the path should go back to its last corner and go round B_2 along the direction that has been selected when the path hit B_1.

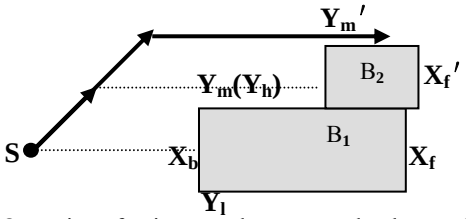


Fig.3. Operation of going round convex and polygon obstacle

a) Tracing out the path

This algorithm recorded each corner of the path in sequence and used a stack to store the tracing direction of these corners. After the searching， the path will be traced out according to the tracing direction of corners.

3. ALGORITHM IMPLEMENTATION

Suppose *s* is source node, *t* is target node, *n* is current node; *X*, *Y*, *dir*, *state* are basic information of a node: coordinate, expanding direction and tracing direction. The basic information of *n* is X_n, Y_n, dir_n, $state_n$; The basic information of *s* is X_s, Y_s, dir_s, $state_s$; The basic information of *t* is X_t, Y_t, dir_t, $state_t$. A stack store the tracing direction of each corner in sequence, so the basic information of top cell *head* is X_{head}, Y_{head}, dir_{head}, $state_{head}$.

Using *count* for the number of nodes that have been searched: initial value of *count* is 0. Each expanding step will let *count* add 1. *Count* will be accessed before each expanding step. If *count* >N*N, the algorithm will be stop and show the fail information.

Xm and *Ym* are coordinates of the extreme of obstacle. The extreme is selected when path going round the obstacle. W_m is the width of obstacle that can be bridged. *Length* is the length of path.

Step1: $s \rightarrow n$. //initalize

Step2: //process of searching path

```
WHILE (Xn≠Xt||Yn≠Yt)
  {
  WHILE (Xn≠Xt) //expanding along horizontal direction
    {
    IF (Xn<Xt)   i=1;
    ELSE   i=－1;
    dirn=3i;
    PUSH (n);
    WHILE (Xn≠Xt && not hit obstacle)
      {expand along dirn, store staten };
    IF (Xn=Xt)
      BREAK;
    IF (hit obstacle) //operation of horizontal expanding
                      //when hit obstacle
      {
      search obstacle's extremes: Yh,Yl,Xb,Xf.;
      IF((Xf－Xb)<Wm & the obstacle can be bridged)
        {
        WHILE (Xn≠Xf)
          { expand along dirn,store staten }
        BREAK;
        }
      ELSE IF (Yl<Yt<Yh)//target node is inside of the
                        //band region of obstacle
        {
        IF(|Yl－Yn|+|Yl－Yt|≤|Yh－Yt|+|Yh－Yn|)
          {
          Ym=Yl;
          j=－1;
          }
        ELSE
          {
          Ym=Yh;
          j=1;
          }
        }
      ELSE IF(Yl>Yt)     //go round with top direction
        Ym=Yl;
        j=－1;
      ELSE        // go round with bottom direction
        Ym=Yh;
        j=1;
      IF(Yl<1)
        Ym=Yh;
        j=1;
      IF(Yh>N)
        Ym=Yl;
        j=－1;
      IF (Yl<1&&Yh>N)
        {stop and show the fail information.}
      n=POP(n);
      decide the value of dirn according to i and j ;
      PUSH (n);
      WHILE(Yn≠Ym－j && not hit obstacle)
        { expand along dirn, store staten }
      IF(Yn=Ym－j)
        operate as figure1—(a)
```

```
            IF(hit obstacle)
              {
               IF(Xn=Xb)   //hit obstacle while expanding
                           //along horizontal direction
                 operate as figure 1—(b);
               ELSE IF(m[Xn－i][Yn]=0)
                  operate as figure 2;
               ELSE
                 operate as figure 2;
              }
          }
      }
    WHILE (Yn≠Yt)     //expanding along vertical direction
      {
       IF(Yn<Yt)
         j=1;
       ELSE
         j=－1;
       dirn=2j;
       PUSH (n);
       WHILE (Yn≠Yt && not hit obstacle)
         { expand along dirn, store staten }
       IF (Yn=Yt)   // operation of vertical expanding
                    //when hit obstacle
          BREAK;
       IF (hit obstacle)
         {same as operation of horizontal expanding when
          hit obstacle；}
      }
  }
```

Step3: the path has been found, show success information.

Step4: (tracing out path)

```
  dirn＝staten;
  WHILE (Xn≠Xs||Yn≠Ys)
    {
     show the coordinate of current node;
     IF(Xn=Xhead && Yn=Yhead)
      dirn= statehead;
      Trace back along dirn; //if |dirn |>3   length+=√2 ;
                             //else        length+= 1;
    }
```

Step5: show the length of path, stop.

4. PERFORMANCE OF ALGORITHM

Suppose a $N\times N$ grid, K is number of obstacles of grid, L is number of obstacles that can be bridged.

Whole searching process is a big circulation. It contains two sub_circulation. If hit a obstacle that must be gone round, the big circulation and one of sub_circulation will be execute once. Searching four extreme of obstacle needs $2N$ steps, for the obstacle's length and width are all shorter of n. The most number of obstacles the searching will hit and do round is $K-L$. Therefore, time complex of the process is $2(K-L)N$. If the searching is fail, the initial direction should be changed and start the searching again. It is same as hitting the first obstacle twice, so time complex of the process is $2(K-L+1)N$.

Tracing process is also a circulation. Its executing times is decided by length of path. Length of path $length<KN$, so the maximal executing times is Kn. Each expanding step needs a executing time. The time of tracing process is KN. Whole time of the process is $(3K-2(L-1))N$. So the time complex of algorithm is $O(3KN)$.

5. CONCLUSIONS

In robot design technique, when robot looking for an avoiding_obstacle path, its expanding direction and moving step are all more flexible than routing of PCB. The running maze algorithm may be improved and use in mobile robot technique. This algorithm fits the constriction of mobile robot's expanding direction. Meantime, length of path can be reduced for it's eight expanding direction. This algorithm speeds up and reduces the searching region. It is an efficient approximately algorithm.

REFERENCES

[1] Jeffrey H. Hoel,"Some Variations of Lee's Algorithm". *IEEE Trans. on Electron. Comput*,Vol.25,No.1,1976, pp.19~24.

[2] Zhang Farong.,"A Searching Algorithm for Approximately Shortest Path Among Obstacles". *Computer Engineering*, Vol.25, No.3,1999,pp.15~16.

[3] Sun Qiaoyu,Pan Yinrong etc,"An Approximately Maze-Algorithm for a Shortest Path with Sparse Obstacles,"*Computer Applications And Software*, Vol.20,No.5, 2003,pp.37~39.

[4] Sun Qiaoyu etc., "A Maze-Algorithm with Eight Directions",*Computer Engineering*,Vol.30, No.1, 2004, pp.90~91.

Qiaoyu Sun is a lecturer of Department of Electronic Engineering, Huaihai Institute of Technology. She graduated from Tianjin University in 1992; from East China Normal University of Science and Computer in 2003 with specialty of application of computer. She has published over 10 Journal papers. Her research interests are grid computing and digital image process.

Yinrong Pan is a professor of Department of Computer Science and Technology, East China Normal University. Doctor leads, He has published over 20 Journal papers. His research interests are computer application and network database.

The Finite Element Simulation of Transmitting Force Way of The Raft Foundation Based on ANSYS*

Qian Lan [1], Yongfeng Du [1], Jun Li [2]
[1]School of Civil Engineering, Lanzhou University of Technology, Lanzhou 730050, China
[2]School of Science, Lanzhou University of Technology, Lanzhou 730050, China
Email: lijun@lut.cn

ABSTRACT

Essential principle and calculation methods are discussed for the simulation of transmitting force way of the raft foundation using topology optimization. Using general-purpose finite element program ANSYS, a three-dimensional finite element model of interaction between raft foundation and soil is established, and a topology optimal model is derived by variable density method. Moreover, the sequential linear programming is chosen to solve the optimal problem. The simulation for the raft foundation of the tall building is conducted. The results show the macroscopic distribution of stress of raft clearly. The research indicates that the topology optimum design by way of FEA is a highly efficient optimum method, which may provides valuable conceptual design idea for raft foundation design of tall building.

Keywords: Transmitting Force Way, Topology Optimal, Variable Density Method, Sequential Linear Programming

1. INTRODCTION

Thick raft foundation is a type of most frequently used foundation in China because it is advantageous both in load bearing and in service ability. Firstly, the thick raft foundation can enhance the bearing capacity and rigidity of foundation and balance the non-uniform settlement of ground. Secondly, it can provide a big underground space that can be used as either underground garage or basement. In addition, compared with the box foundation, the thick raft foundation has the advantages of low cost and the fast speed of executes of works. However, thick raft is a kind of very expensive foundation, applying it into manufacturing means not only concrete consuming, but also needs large amounts of steel for reinforcement. An accurate analysis is helpful for a better understanding of force distribution in a thick raft, thus a reasonable design. The analysis of thick raft is usually more complicated because the no more applicable[1]. This paper investigates the local distribution nature of the bending moment near the bottom of effect of shear deformation in thick raft is very significant, and the Kirchhoff theory used for ordinary thin plate is shear wall and columns. A Mindlin model for moderate thickness plate is used to improve the accuracy of calculation. For this purpose, general-purpose finite element software, ANSYS is employed, and a 3-D finite element model of interaction between the raft foundation and soil is established. A topology optimal model is derived using variable density method, and the sequential linear programming is chosen to solve the optimal problem. The numerical examples show that the optimal method presented in this paper is feasible and effective. The result of topology optimization reflects the law of load transferring from raft to foundation and clearly reveals the part of the raft where the reinforcement needs to be enhanced.

*Supported by the National Natural Science Foundation of China under Grant No.10331010 and the Outstanding Youth Foundation of Lanzhou University of Technology.

2. TOPOLOGICAL OPTIMIZATION MODEL AND SOLUTION

2.1 Topological Optimization Model

Variable Density Method (VDM) is commonly used for topological optimization of continuum structure[3]. The main idea of VDM is to introduce an imaginary material with variable density. A base structure is first defined the degree of existence of each finite element is described using pseudo density which is associated with the stress level. When the density of the element is equal to zero, there is no material in this element. So the element should be deleted. While the density of the unit is equal to one, there is material in this element. So the unit should be kept. The density of material is regard as the variable for topological optimization. Therefore, the topological optimization design is thus changed into the material optimum distribution problem.

In the Variable Density Method, the density of each finite element is chosen as the topological optimization variable, and the stiffness of material is taken as the objective function. The topological optimization model is shown as following: find the density variables $\{\rho\}^T = \{\rho_1, \rho_2 \cdots \rho_{n_e}\}$ such that

$$\text{Min } C(\rho) = U^T(\rho)F = U^T(\rho)K(\rho)U(\rho) \quad \text{Eq. (1)}$$

$$\text{Subject to } H(\rho) = \sum_{i=1}^{n_e} \int_{\Omega_i} \rho_i d\Omega_i - M_0 \le 0 \quad \text{Eq. (2)}$$

$$K(\rho)\cdot U - F = 0 \quad \text{Eq. (3)}$$

$$\varepsilon \le \rho_i \le 1, \qquad 0 < \varepsilon << 1 \quad \text{Eq. (4)}$$

where $C(\rho)$ is the objective; $H(\rho)$ is constraint; F is loading matrix of the nodes; U is the displacement matrix of nodes; M_0 is the mass constraint; n_e is the total number of elements; Ω_i is the integral area of units; ρ is the density matrix.

The stiffness matrix of material is shown as:

$$K(\rho) = \sum_{i=1}^{ni} K_i(\rho_i) = \sum_{i=1}^{ni} \int B_i^T D(\rho_i) B_i d\Omega$$

$$\rho = \{\rho_i\}^T \quad (i = 1,2\cdots n_e) \quad \text{Eq. (5)}$$

$$D(\rho_i) = \frac{E(\rho_i)}{1-\nu^2}\begin{bmatrix} 1 & \nu & 0 \\ \nu & 1 & 0 \\ 0 & 0 & \frac{1-\nu}{2} \end{bmatrix}$$

$$E(\rho_i) = E_0 \rho_i^n \quad \text{Eq. (6)}$$

where B_i is the matrix of relationship between the stress and the displacement; $n = 3 \sim 9$; ρ_i should be satisfied with $\varepsilon \le \rho_i \le 1$ and $0 < \varepsilon << 1$; E_0 is the modulus of elasticity.

2.2 Solution

The sensitivity of the objective function and the constraints is shown that

$$\frac{\partial C}{\partial \rho_i} = -U^T \frac{\partial K}{\partial \rho_i} U + \frac{\partial U^T}{\partial \rho_i} KU + U^T K \frac{\partial U}{\partial \rho_i} \quad \text{Eq. (7)}$$

$$\frac{\partial H}{\partial \rho_i} = \int_{\Omega_i} d\Omega \quad \text{Eq. (8)}$$

According to Eqs. (4), the equation can be derived as

$$\frac{\partial K}{\partial \rho_i} U = -K \frac{\partial U}{\partial \rho_i} \quad \text{Eq. (9)}$$

The equivalent form of the sensitivity of the objective function and the constraints can be derived from Eqs. (7), (9).

$$\frac{\partial C}{\partial \rho_i} = -U_i^T \frac{\partial K_i}{\partial \rho_i} U_i = -\frac{n}{\rho_i} U_i^T K_i U_i = -\frac{2n}{\rho_i} \times$$

(the deformational energy of the unit) Eq. (10)

Because the number of variable for topological optimization of the base structure is large, the computation becomes complicated. Proper optimization method having good convergence speed and reliable optimization result must be chosen. Sequence of Linear Programming is very capable of dealing with large number of the design variable. This method is a kind of optimization method used extensively in structure optimization design at present. In this method, the objective function and the constraints are linearized by taking the first terms of the Taylor series expansion about the current iteration point. The original NLP problem is locally approximated by linear terms. This LP problem can be solved repeatedly, redefining the new iteration point each time as the optimal solution of the previous problem. In order to improve computational efficiency, the simplex is selected to solve the LP problem.

3. EXAMPLE

3.1 Project Introduction

A structure that consists of 2 basement floors and two towers with 29 stories each is chosen as the numeral example. Its foundation is the raft and the superstructure is framed-tubes. The dimensions of raft are 32m×12m×1.8m. The sizes of two tubes are 8m ×8m and 8m ×7m respectively. The loads produced by tubes are 90743KN and 141941KN respectively and the linear load produced by is outer wall 1200KN/m.

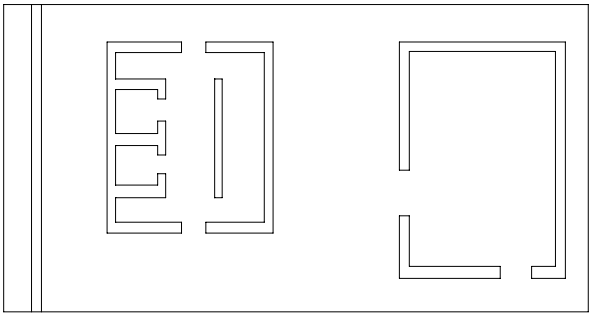


Fig.1. Plan of the raft

A part of raft including two tubes (the plan was shown in Fig. 1) was taken out in this paper. In order to simulate the action of the adjacent raft, the support conditions of the long sides of the raft ribbon are slide support. The topological optimization was carried on.

3.2 The Analysis of Raft

The analysis of thick raft is usually more complicated because the effect of shear deformation in thick raft is very significant, and the Kirchhoff theory used for ordinary thin plate is no more applicable. Eight-nodes isoparametric finite elements were used to simulate the reinforced concrete in raft. Mindlin model for moderate thickness plate in which transverse shear is considered in order to improve the accuracy of calculation is used. The steel reinforcements were spread in whole space of concrete. This method has advantages of the simple model and the high precision of calculation.

3.3 Soil Model

Selecting a reasonable model for soil is important for analysis of interaction. It not only affects the distribution of the foundation reaction, but also affects the internal force and deformation of foundation and superstructure. Soil can be stratified and regarded as even, continuous, isotropism in every layer. The stratified soil is simulated as 20 nodes isoparametric finite elements that can realize the comparatively true soil body state with smaller calculation amount.

When the finite element model of interaction between raft foundation and soil was established, some principles were considered in this paper as followings:

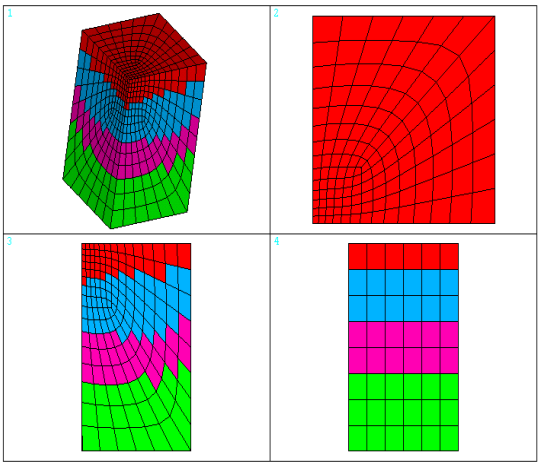


Fig.2. Meshing of uneven and layered soil

(1) In order to improve the computation accuracy with less computational effort, the meshes of the area under the raft are smaller than that of other area because the stress of this area is concerned most. (Shown in Fig.1)
(2) Make sure that different material attribute is assigned to each layer of the soil. (Shown in Fig.1)
(3) Try to guarantee all finite elements are regular.
(4) The dimensions (a, b, H) of the soil are chosen according to the scope of loading effect. The boundary conditions are shown as Fig.2. The displacement of the surface of soil can be described as $u|_{x=0} = 0$、$u|_{x=a} = 0$、$\tau_{xz}|_{x=0} = 0$、$\tau_{xz}|_{x=a} = 0$、$v|_{x=0} = 0$、$v|_{x=a} = 0$、$\tau_{yz}|_{x=0} = 0$、$\tau_{yz}|_{x=a} = 0$. However, the displacement of bottom of soil is regarded as zero.

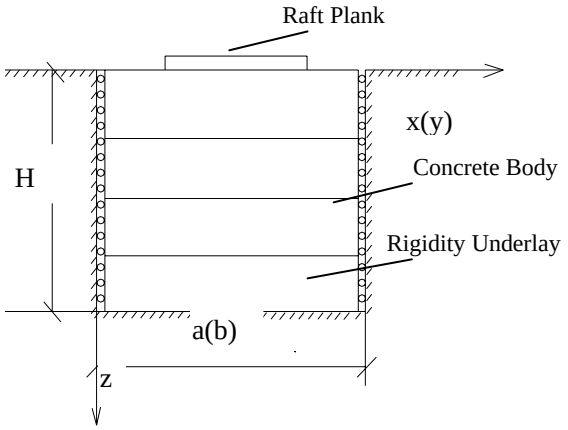


Fig.3. Model of soil

3.4 Finite Element Equation

Finite element equation of interaction between foundation and soil is shown as following:

$$[K_R + K_S]\{U\} = \{Q\} \qquad \text{Eq. (11)}$$

where $[K_R]$ is the stiffness matrix of the raft; $[K_S]$ is the stiffness matrix of soil; $\{U\}$ is the displacement vector; $\{Q\}$ is the load vector. This Finite element equation is solved by Newton-Raphson iterations. Compared with other methods, the work done for this approach is less and satisfactory results were gained.

3.5 Results of the Topological Optimization

Fig.4 indicates the result of the topological optimization. The dark color represents the bigger value of the pseudo density, corresponding to big stress in the figure. Some principles can be revealed from the result of the topological optimization:

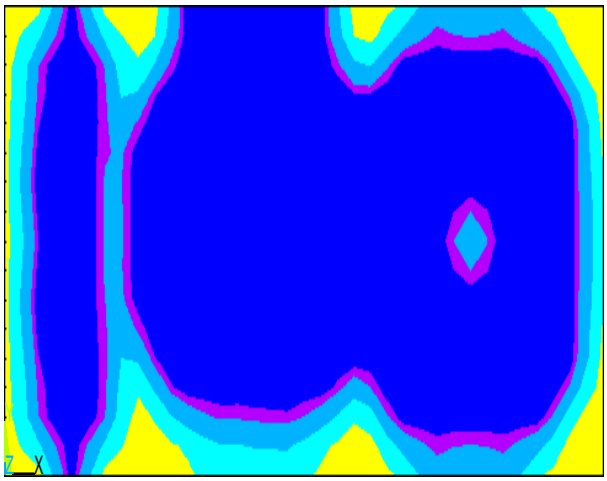


Fig.4. Optimal result

(1) Because the loading provided by tubes are great, the stress of the raft under the two tubes is bigger than other positions. Compared with the right tube, the left tube has the smaller size and the heavier loads, and there are no internal shear walls. For this reason, the stress of the raft of the left tube is distributed evenly in the edge and the interior of the tube. However, the phenomenon of uneven stress within the right tube appeared. Because of a short distance between two tubes, the stress of the raft between two tubes is also great relatively. This fact can be reflected in the testing results of the stress of the reinforcements. So, the reinforcements of this part of raft need to be enhanced. In addition, the reasonable locations of tubes are important for the structural design.

(2) In spite of the large stress of the exterior wall, the stress of the part between tube and the exterior wall is small. Compared to the loads provided by tube, the loads provided by the exterior wall is heavier. According to the shortest route principles for loading transmission, the stress of the raft between the tube and the outer wall is smaller than that of the raft between two tubes.

(3) From the results of the topological optimization, it can be founded that the stress of the edge of the raft is the smallest. So, it is important that a suitable distance between the edge and the outer wall should be kept.

4. CONCLUSIONS

Using general-purpose finite element program ANSYS, a three-dimensional finite element model of interaction between raft foundation and soil is established, and a topology optimal model is derived by variable density method. Moreover, the sequential linear programming is chosen to solve the optimal problem. Some Conclusions can be drawn as following:

(1) Compared with conventional method, the topological optimization method based on the finite analysis improves the computational accuracy and the high quality of design.

(2) The result of topology optimization reflects the law of load transferring from raft to foundation.

(3) The result of topology optimization can clearly reveals the part of the raft where the reinforcement needs to be enhanced.

REFERENCES

[1] JIANG Fuxiang, WANG Yutian, “Superstructure-Thick raft-Soil Interaction Analysis,” *Soil Eng. and Foundation*, 1998,12(9), 6:10

[2] DU Yongfeng, Wang Yongqi, LI Ya’e, “Optimum Design of Box Foundation Considering Interaction with Frame-Shear- Wall Structure,” *OPTIMIZATION OF CAPITAL CONSTRUCTION*, 2000, 20(2), 19:22

[3] WANG Jian, CHENG Gendong, “Optimal Topology Design of Thin Plate with Stress Constraints,” *ACTA MECHANICA SOLIDA SINICA*, 1997,18(12),317:322

[4] YUAN Zhen, WU Changchun, ZHUANG Shoubing, “Topology Optimization of Continuum structure Using Hybrid Elements and Artificial Material Model,” *JOURNAL OF CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY*, 2001, 31(12) 694:699

[5] JIANG Yunzheng, QU Shuying, CHU Mingjin, “Topological Optimization of continuum structures,” *Chinese Journal of Computational Mechanics*, 2003, 20(4), 146:154

Lan Qian is an assistant professor of School of Civil Engineering , Lanzhou University of Technology. She graduated from Lanzhou University of Technology in 2004 and obtained his Master degree. She has published over 10 Journal papers. Her research interests are in reasoning about knowledge, uncertainty reasoning

and non-classical mathematical logic.

Yongfeng Du is a professor of School of Civil Engineering , Lanzhou University of Technology. He graduated from Dalian University of Science and Technology in 2004 and obtained his Doctor degree. He has published over 80 Journal papers. His research interests are Control Algorithm , Smart IsolatedStructure, the structural health monitoring.

Jun Li is an assistant professor of School of Science , Lanzhou University of Technology. He graduated from Shaanxi Normal University in 2002 and obtained his Master degree. And now, he is a graduate studying in the college of mathematics and information science, Shaanxi Normal University, majored in Uncertainty reasoning, expecting to receive his Ph.D one year later. He has published over 30 Journal papers. His research interests are in reasoning about knowledge, uncertainty reasoning and non-classical mathematical logic.

Distributed/Parallel Applications

Wildland Fire Simulation with Sensor Network Data Correction*

Craig C. Douglas[1], Jonathan Beezley[2], Jan Mandel[2]
Janice Coen[3], Guan Qin[4], Anthony Vodacek[5]
[1]University of Kentucky, Computer Science Department Lexington, KY, USA
[2]University of Colorado at Denver and Health Sciences Center, Mathematics Department Denver, CO, USA
[3]National Center for Atmospheric Research Boulder, CO, USA
[4]Texas A&M University College Station, TX, USA
[5]Rochester Institute of Technology, Imaging Science Department Rochester, NY, USA
Email: douglas-craig@cs.yale.edu

ABSTRACT

We report on an ongoing effort to build a Dynamic Data Driven Application System (DDDAS) for short time frame prediction of weather and wildfire behavior from real time weather data, images, and sensor streams. The system changes its predictions as new data is received. We use a single long term running simulation that corrects itself using out of order, imperfect sensor data. The DDDAS version replaces a code that was previously run using data only with static initial conditions. DDDAS entails the ability to dynamically incorporate additional data into an executing application, and in reverse, the ability of an application to dynamically steer the measurement process. Visualization in the field is an important aspect.

Keywords: Fire Tracking, Dynamic Data-driven Application Systems, Sensor Networks, Adaptive Computing, Parallel Computing.

1. INTRODUCTION

We describe the current state of a dynamic data driven application system (DDDAS) for simulating wildland fires.

DDDAS is a paradigm whereby an application (or simulation) and its underlying measurements become a symbiotic feedback control system. DDDAS entails the ability to dynamically incorporate additional data into an executing application, and in reverse, the ability of an application to dynamically steer the measurement process. Such capabilities promise more accurate analysis and prediction, more precise controls, and more reliable outcomes. The ability of an application to control and guide the measurement process and determine when, where, and how it is best to gather additional data has itself the potential of enabling more effective measurement methodologies. Furthermore, the incorporation of dynamic inputs into an executing application invokes new system modalities and helps create application software systems that can more accurately describe real world, complex systems. This enables the development of applications that intelligently adapt to evolving conditions and that infer new knowledge in ways that are not predetermined by the initialization parameters and initial static data.

The motivation for our research is the following:

- Improving society with a more accurate prediction compounded with the inherent challenge in modeling nonlinear, rapidly changing phenomena.
- The difficulty in obtaining remote or in situ data.
- The challenges of communicating the on site, out of sequence data of unknown quality to remote supercomputers and using it to steer simulations and data acquisition.

The research extends well beyond the data assimilation work in progress in atmospheric or ocean sciences due to the specific application challenges: the model is strongly nonlinear and irreversible, the data arrives out of sequence from disparate data sources, and error distributions simply are not close to Gaussian. Our DDDAS is built upon previously existing models and codes with significant additional code and new algorithms.

Components have been developed and added to the coupled atmosphere-wildfire model which contains the following:

- Save, modify, and restore the state of the model.
- Apply ensemble data assimilation algorithms to modify ensemble member states by comparing the data with synthetic data of the same kind created from the simulation state.
- Retrieve, process, and ingest data from both novel ground based sensors and airborne platforms in the near vicinity of a fire.
- Provide computational results visualized in several ways adaptable to user needs.

DDDAS requires sensors capable of dynamically supplying data to a simulation. An ideal sensor is sensitive, selective, and able to communicate high level spatial, temperature, and chemical information to the simulation rapidly using negligible bandwidth.

Integrated Sensing and Processing (ISP) aims to replace current sensor designs with such DDDAS optimized sensor system architectures, comprising interdependent networks of functional elements, each of which may span the roles and functions of multiple separate subsystems in present generation sensor systems. ISP simplifies sensing in DDDAS through spanning those multiple roles and functions. ISP research is developing mathematical tools that facilitate the design and global optimization of systems that interactively unite usually independent functions of sensing, signal processing, communication, and exploitation. ISP achieves diminution of crucial degrees of freedom in sensing system design and operation without regard to traditional subsystem limits and interconnect structures. This reduction is realized by applying modern systematic methods from physics based computational modeling and fast data adaptive representations to discover and take advantage of structure present in the data across every stage of the sensor system. In many instances, ISP enables an instantaneous dimensionality reduction to a tractable optimization problem that is far more deferential to the end to end structure of the problem than the traditional sensing approach.

* Supported in part: NSF grants CNS-0540178, EIA-0218229, ACI-0324876, OISE-0405349, and ACI-0305466.

Data that come into the data center must go through a process consisting of up to six steps.

1. *Retrieval*: Get the data from sensors. This may mean receiving data directly from a sensor or indirectly through another computer or storage device (e.g., a disk drive).
2. *Extraction*: The data from some sensors may be quite messy in raw form, thus the relevant data may have to be extracted from the transmitted information.
3. *Conversion*: The units of the data may not be appropriate for our application.
4. *Quality control*: Bad data should be removed or repaired if possible. Missing data (e.g., in a composite satellite image) must be repaired.
5. *Store*: The data must be archived to the right medium (or media). This might mean a disk, tape, or computer memory, or no storage device at all (or only briefly) if data is not being archived permanently or only temporarily.
6. *Notification*: If a simulation is using the data as it comes into the data center, the application needs to be informed of the existence of new data.

ISP simplifies DDDAS by performing data extraction and data conversion at the detector in the sensor, eliminating steps 2 and 3 in the previous paragraph. ISP also presents the data as high level information tokens that require very little communication bandwidth. Bad data may be edited or removed as data are tokenized, potentially eliminating step 4 in the data center as well.

2. WILDLAND FIRE MODEL

The original modeling system is composed of two parts: a numerical weather prediction model and a fire behavior model that models the growth of a wildfire in response to weather, fuel conditions, and terrain [8, 9]. These models are two way coupled so that heat and water vapor fluxes from the fire are released into the atmosphere, affecting the winds in particular, while the fire affected winds feed back upon the fire propagation. This wildfire simulation model can thus represent the complex interactions between a fire and the atmosphere.

The meteorological model is a three dimensional non-hydrostatic numerical model based on the Navier-Stokes equations of motion, a thermodynamic equation, and conservation of mass equations using the anelastic approximation. Vertically stretched terrain following coordinates allows the user to simulate in detail the airflow over complex terrain. Gridded national weather forecasts are used to initialize the domain and update lateral boundary conditions. Two way interactive nested grids capture the outer forcing domain scale of the synoptic scale environment while allowing the user to telescope down to tens of meters near the fireline through horizontal and vertical grid refinement. Weather processes such as the production of cloud droplets, rain, and ice are parameterized using standard treatments.

In the original model, local fire spread rates depend on the modeled wind components, fuel properties, and terrain slope through an application of the semi-empirical Rothermel fire spread formula [10]. We are replacing the Rothermel model with a simple physics and PDE based model [11]. This PDE model uses the reaction-convection-diffusion equation for the temperature and fuel supply. This simple model is capable of producing a reasonable fire behavior with an advancing fire front. A more advanced version of this model is under development, which will include several species of fuel, radiative heat transfer between fuel species, and evaporation of moisture. It is anticipated that this model will replace the empirical fire model and it will be coupled to the atmospheric model. Some related physics based fire models in the literature are in [12, 13].

Prediction with the coupled atmosphere fire model is achieved using an Ensemble Kalman Filter (EnKF). Ensemble filters work by advancing in time a collection of simulations started from randomly perturbed initial conditions. When the data is injected, the ensemble (called *forecast*) is updated to get a new ensemble (called *analysis*) to achieve a least squares fit using two conditions: the change in the ensemble members should be minimized, and the data should fit the ensemble members state. The weights in the least squares are obtained from the covariances of the ensemble and of the data error. For comprehensive surveys of EnKF techniques, see [14, 15, 16]. In general, EnKF works by forming the analysis ensemble as linear combinations of the forecast ensemble.

We are using filters based on the EnKF with data perturbation [17]. But, even with a highly simplified wildfire model, the data assimilation produces an ensemble with nonphysical solutions causing the simulations to break down numerically. Breakdown occurs much sooner with the full model. Therefore, we use a regularization by adding a term involving the change in the spatial gradient of ensemble members to the least squares [18]. Existing ensemble filter formulas assume that the observation function is linear and then compute with the observation matrix. We derived a mathematically equivalent ensemble filter that just needs to evaluate the observation function for each ensemble member, which simplifies the code.

We use system states that combine states at several times [11] for assimilating of out of order data that we use. Our parallel computing framework was designed knowing we would have to deal with out of order data injection.

Data comes from fixed ground sensors that measure temperature, radiation, and local weather conditions [19]. These systems will survive burn-over by low intensity fires and are intended to supplement other sources of weather data derived from permanent and portable automated weather stations. The temperature and radiation measurements provide the direct indication of the fire front passage and the radiation measurement can also be used to determine the intensity of the fire.

Data also come from images taken by sensors on either satellites or airplanes. The primary source of image data is the Wildfire Airborne Sensor Project (WASP) [20]. This three wavelength digital infrared camera system is carried on an airplane that is flown over the fire area. Camera calibration, an inertial measurement unit, GPS, and digital elevation data are used in a processing system to convert raw images to a map product with a latitude and longitude associated with each pixel. The three wavelength infrared images can then be processed using a variety of algorithm approaches [20, 21] to extract which pixels contain a signal from fire and to determine the energy radiated by the fire [22, 23].

The data are related to the model by the observation equation. The observation function maps the system state to *synthetic data*, which are the values the data would be in the absence of

modeling and measurement errors. Knowledge of the observation function, the data, and an estimate of the data error covariance is enough to find the correct linear combinations of ensemble members in the ensemble filter. For an observation function that is simply the value of a variable in the system state, the natural choice of approximate inverse can be just the corresponding term of the data residual, embedded in a zero vector.

Building the observation function and its approximate inverse requires conversion of physical units between the model and data and conversion and interpolation of physical coordinates. In addition, synthetic data at instants of time between the simulation time of ensemble members need to be interpolated to the data time. The data injection itself is done by updating the ensemble to minimize a weighted sum of the data residual and the change in the ensemble.

The data items enter in a pool maintained by the data acquisition module. The assimilation code can query the data acquisition module to determine if there are any new data items available, request their quantitative and numerical properties, and delete them from the pool after they are no longer needed.

Visualization of the model output as an image is accomplished by brightness, color encoding, and transparency for a visual indication of the location and intensity of the fire, and of the probability distribution of the prediction. 3D visualization of the fire is more complex and complexity increases if high spatial resolution of the output is desired. 3D visualization uses model output from the fire propagation code for the flame region and from the atmospheric code for visualization of smoke. Ensemble statistics are used for visualization of probability.

The geographic output of the fire model in 2D or 3D is visualized in a number of ways. A PDF file of the output as a map is generated for potential output as hardcopy view of the fire at a set point in time. For computer based mapping, manipulation, and visualization of the model output, file formats compatible with the geographic information system (GIS) products are generated.

The time varying output for both 2D and 3D is also used to generate a movie playable in any of the media formats, e.g., MPEG. The user may select movie duration up to the maximum extent of the model prediction.

An intuitive and easy method for map visualization is to use a web based mapping server, e.g., GIS software, Google Maps, or Google Earth. These web based programs simplify access to map and image data. They let us display model output movies on top of a relevant map background. Within Google Earth, for example, this allows user control of the viewing perspective, zooming into specific sites, and selecting the time frame of the visualization within the parameters of the current available simulation. These web based programs also allow switching between background types, for example, USGS topographic maps or high resolution satellite images with a road layer or other pertinent layers such water sources added.

3. CONCLUSIONS

All DDDAS share numerous common features:

- The correct sensor needs to be chosen to get the right data at a given time.
- The sensors must be placed in the right locations
- Data is not necessarily accurate nor does it arrive on time in the correct order. Hence, data must be filtered before use and error distributions in the data must be known and available for use.
- The sensors should be reprogammable in some sense directly by the application.
- The potential for rapid error growth without data steering.
- The application's models, numerical methods, and major item to be tracked may need to be changed as a result of the incoming sensor data or a human in the loop.
- Long term simulations are possible using dynamic data instead of having to run many short term ones with incoming, but static initial guesses.

A challenge is to develop common frameworks that work on multiple types of DDDAS codes.

One of short term goals is a full computational test. Data will move, possibly unreliably, from remote sensors to a remote computational machine. Our simulations will be data-driven in terms of the models and scales we use. The choices of models and scales will be made in part based on the data streaming in. We are now in a position to develop the final piece of our DDDAS strategy: having the simulation control how much data is needed and from where in order to improve the quality of the flame wave front predictions. Only then will we have a truly symbiotic relationship between the running computations and data collection. Our current test should have the right ingredients to predict how our DDDAS will work in a planned future field test with a real wildland fire.

REFERENCES

[1] http://www.dddas.org includes project descriptions, many DDDAS workshop virtual proceedings, and links to DDDAS software.

[2] K. Baldridge, G. Biros, A. Chaturvedi, C. C. Douglas, M. Parashar, J. How, J. Saltz, E. Seidel, A. Sussman, January 2006 DDDAS Workshop Report, National Science Foundation, 2006, http://www.dddas.org/nsf-workshop-2006/wkshp_report.pdf.

[3] 2003 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science - ICCS 2003: 3rd International Conference*, Melbourne, Australia and St. Petersburg, Russia, June 2-4, 2003, Proceedings, Part IV, P.M.A. Sloot, D. Abramson, A.V. Bogdanov, J.J. Dongarra, A.Y. Zomaya, Y.E. Gorbachev (Eds.), Lecture Notes in Computer Science, Vol. 2660, Springer-Verlag Heidelberg, 2003, pp. 279-384.

[4] 2004 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science - ICCS 2004: 4th International Conference*, Kraków, Poland, June 6-9, 2004, Proceedings, Part III, Marian Bubak, Geert Dick van Albada, Peter M. A. Sloot, and J.J. Dongarra (eds.), Lecture Notes in Computer Science series, vol. 3038, Springer-Verlag Heidelberg, 2004, pp. 662-834.

[5] 2005 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science - ICCS 2005: 5th International Conference*, Atlanta, Georgia, USA, May 22-25, 2005, Proceedings, Part II, Vaidy S. Sunderam, Geert Dick van Albada, Peter M.A. Sloot, Jack J. Dongarra (eds.), Lecture Notes in Computer

Science series, vol. 3515, Springer-Verlag Heidelberg, 2005, pp. 610-745.

[6] 2006 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science – ICCS 2006: 6th International Conference*, Reading, UK, May 28-31, 2006, Proceedings, Part III, edited by V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, and J.J. Dongarra, Lecture Notes in Computer Science 3993.

[7] C. C. Douglas, A. Deshmukh, M. Ball, R. E. Ewing, C. R. Johnson, C. Kesselman, C. Lee, W. Powell, R. Sharpley, "Dynamical data driven application systems: Creating a dynamic and symbiotic coupling of application/simulations with measurements/ experiments," National Science Foundation, Arlington, VA, 2000. http://www.dddas.org/nsf-workshop-2000/worksop_report.pdf.

[8] T.L. Clark, J.L. Coen, and D. Latham, "Description of a coupled atmosphere-fire model," Intl. J. Wildland Fire, 13 (2004), pp. 49-64.

[9] J.L Coen, "Simulation of the Big Elk Fire using using coupled atmosphere-fire modeling," Intl. J. Wildland Fire, 14 (2005), pp. 49-59.

[10] R.C Rothermel, "A mathematical model for predicting fire spread in wildland fires," *USDA Forest Service Research Paper* INT-115, January, 1972.

[11] J. Mandel, M. Chen, L.P. Franca, C. Johns, A. Puhalskii, J.L. Coen, C.C. Douglas, R. Kremens, A. Vodacek, and W. Zhao, "A note on dynamic data driven wildfire modeling," in *Computational Science - ICCS 2004*, M. Bubak, G.D. van Albada, P.M. A. Sloot, and J.J. Dongarra (eds.), Volume 3038 of Lecture Notes in Computer Science, Springer-Verlag, 2004, pp. 725-731.

[12] R. Linn, J. Reisner, J.J. Colman, and J. Winterkamp, "Studying wildfire behavior using FIRETEC," Int. J. Wildland Fire, 11 (2002), pp. 233-246.

[13] F.J. Seróon, D. Gutiérrez, J. Magallón, L. Ferragut, and M.I. Asensio, "The evolution of a WILDLAND forest FIRE FRONT," *Visual Computer*, 21 (2005), pp. 152-169.

[14] G. Evensen, The ensemble Kalman filter: "Theoretical formulation and practical implementation," *Ocean Dynamics*, 53 (2003), pp. 343-367.

[15] G. Evensen, 'Sampling strategies and square root analysis schemes for the EnKF," *Ocean Dynamics*, 2004, pp. 539-560.

[16] M.K. Tippett, J.L. Anderson, C.H. Bishop, T.M. Hamill, and J. Whitaker, "Ensemble square root filters," *Monthly Weather Review*, 131 (2003), pp. 1485-1490.

[17] G. Burgers, P.J. van Leeuwen, and G. Evensen, "Analysis scheme in the ensemble Kalman filter," *Monthly Weather Review*, 126 (1998), pp. 1719-1724.

[18] C.J. Johns, and J. Mandel, "A two-stage ensemble Kalman filter for smooth data assimilation, environmental and ecological statistics," in *Conference on New Developments of Statistical Analysis in Wildlife, Fisheries, and Ecological Research*, Oct 13-16, 2004, Columbia, MI.

[19] R.L. Kremens, J. Faulring, A. Gallagher, A. Seema, and A. Vodacek, "Autonomous field-deployable wildland fire sensors," *International J. of Wildland Fire*, 12 (2003), pp. 237-244.

[20] Y. Li, A. Vodacek, R.L. Kremens, A. Ononye, and C. Tang, "A hybrid contextual approach to wildland fire detection using multispectral imagery," *IEEE Trans. Geosci. Remote Sens*., 43 (2005), pp. 2115-2126.

[21] J. Dozier, "A method for satellite identification of surface temperature fields of subpixel resolution," *Remote Sens*. Environ., 11 (1981), pp. 221-229.

[22] M.J. Wooster, B. Zhukov, and D. Oertel, "Fire radiative energy for quantitative study of biomass burning: derivation from the BIRD experimental satellite and comparison to MODIS fire products," *Remote Sensing of Environment*, 86 (2003), pp. 83-107.

[23] A.M.S. Smith, M. Wooster, N. Drake, G. Perry, F. Dipotso, M. Falkowski, and A. Hudak, "Testing the potential of multi-spectral remote sensing for retrospectively estimating fire severity in African savanna environments," *Remote Sens*. Environ., 97 (2005), pp. 92-115.

Craig C. Douglas is a professor of computer science and mechanical engineering at the University of Kentucky and a senior research scientist of computer scientist at Yale University. He has also held positions at Duke University and the IBM Thomas J. Watson Research Center. He will be on sabbaitical at Texas A&M during the 2007-2008 academic year. He has a Ph.D. (1982), M.Phil. (1980), and M.S. (1978) in computer science from Yale University and an A.B. (1977) in mathematics from the University of Chicago.

Jonathan Beezley is a graduate student and **Jan Mandel** is a professor of mathematics at the University of Colorado at Denver and Health Sciences Center. **Janice Coen** is a research scientist at the National Center for Atmospheric Research (NCAR). **Guan Qin** is the associate director of the Institute for Scientific Computation at Texas A&M University. **Anthony Vodacek** is an associate professor of imaging science at the Rochester Institute of Technology.

Flight Cast – An Airline Flight Delay Predicting DDDAS *

Ray Hyatt , Jr.[1], Divya Bansal[1], Soham Chakraborty[1], Jay Hatcher[1], Chun-Lung Lim[1], Gundolf Haase[2]
[1]C. Mark Maynard, Trevor Presgrave, and Craig C. DouglasComputer Science Department, University of Kentucky Lexington, KY, USA
[2]Mathematics Department, Karl-Franzens University of Graz Graz, Austria
Email: [1]rhyatt@stdio.com ,[1]douglas-craig@cs.yale.edu

ABSTRACT

Each year approximately twenty percent of flights in the U.S. are delayed, costing large sums of money in terms of lost business opportunities and wasted time. We propose to develop a dynamic data-driven application system (DDDAS) to track the results of airline flights over time and use this data to accurately predict the probability of delay or cancellation of a flight. Initially the factors taken into account included: weather, terrorism threat level as reported by the FAA, and the flight information provided by the airlines. As more data is collected we expect that seasonal trends could also be detected and added to the model.

Keywords: Dynamic Data-driven Application System, Air Travel, Weather, Flight Prediction.

1. APPROACH

This project started as a joint class project in dynamic data-driven application systems (DDDAS) [1-7] course. Our approach is divided into several smaller sub-projects. These were produced along the lines of the overall model as depicted in Fi.1. The work falls into one of these categories:

1) Sensors: collect data for the DDDAS.
2) Transport: transfer data between the sensors and the other parts of the DDDAS.
3) Data store: central repository for collected data.
4) Predictor: predict flight delay and cancellation based on historical data and current conditions.
5) Corrector: analyze the accuracy of predictions and make corrections to the predictor to improve accuracy over time.

The DDDAS needs at least one element from each of the above to function but works and even benefits from having multiples of each.

1.1 Delta Airlines Sensor

This sensor collects data from the Delta Airlines' website [9] and reformats it into a form suitable for use by our various tools.

The Delta Airlines sensor had several interesting challenges in its evolution to the current state. The first challenge in the prototype was getting the data from the Delta website. No API was found, so we had to look for some viable alternative. After some experimenting, a URL was discovered that permitted placing the date and flight number directly into the URL, resulting in the browser fetching the desired information from the website without having to bother with forms or other input. This worked fine for browsers, but it caused problems initially in command line tools like fetch or wget. It was discovered that this was due to the various cookies the website was setting. After isolating that cookie it was possible to configure wget to fetch pages reliably. Once the web page was collected it was piped through a number of regular expressions via grep to pick out the interesting parts and to exclude the unwanted data. This proved that it could be done, so we moved to implementation of a production model in Python.

Python [9] was chosen as our default tool language due to strong lobbying our class discussions after researching what libraries where available that made our tasks easier. (Though later, many other languages where incorporated in the various pieces of the overall project.) A key library is mechanize, which neatly wraps up the entire URL fetching process into a single command and bypasses the manual cookie handling which had plagued the prototype sensor. The initial version of the sensor also used libxml2dom to assist in stripping the html and xml formatting from the page. Due to problems in date handling and Delta's changes to its website, it was dropped from the final version.

The initial version of Delta sensor outputted a comma separated value (CSV) list for each flight. This data was stored in a log until the data design was firmed up. Once the data store format became available we wrote a perl script to transform it into a series of insert statements for postgres sql. Since it was in comma separated value form, (CSV), this could have been converted or imported in a number of other ways, but we needed to rewrite the flight field and the airport fields to match the final format of the data store so we used perl to do all of these at once.

Delta overhauls their website periodically, changing the format of the pages, and completely breaking the Delta sensor. A change recently, coupled with a finalization of the data format in the data store, prompted major changes to the Delta sensor design. Specifically, we reduced the Python portion of the Delta sensor, via heavy commenting, to fetching the URL, generating the timestamp, and then outputting this to standard out only. This output can be redirected to a file or piped to another program in typical UNIX command line fashion. We modified the Makefile for the project to have several new build stanzas, specifically ones to take a collection of flights from a file and generate either flat text output files or postgres insert statements which can be appended to a master insert file. That file could then be loaded into the database via a simple \i filename on the postgres command prompt. It would not be difficult to have these directly loading into the database but since remote connectivity to the database was difficult, with a firewall blocking access, this seemed like a reasonable workaround. A sensor running on the same box with the database should have no problems with the firewall and could deliver that data directly to the data store.

1.2 United Sensor

To begin data retrieval from United Air Lines [10], a Python script is used to gather the information from the website. We again use the mechanize package for web browsing to get the

* Supported in part: NSF grants CNS-0540178, EIA-0218229, ACI-0324876, OISE-0405349, and ACI-0305466.

html from the United website. Each segment of a flight is gathered from a separate URL request with differing destination and origin airport codes.

Once the web page is downloaded and placed into a string we use regular expressions to filter out the relevant data. As the pertinent information is placed deep inside layers of html each parameter often is parsed in several successive steps.

As United does not always display the information required the value unknown is used as a default for missing data.

The United Sensor can currently gather flight information for individual legs of the flight through URL requests and insert them into the database. It has limited error handling with some of the fields having the default value of unknown. The sensor is meant to be called by an external program either on demand or by a scheduling tool such as a cron.

1.3 Weather Sensor

One of the avenues explored was Yahoo!'s weather service [11]. This service is very developer friendly and provides a plethora of data based on zip code.

Yahoo! provides RSS feeds for their weather reports and forecasts. On their developer network they even provide a tutorial on accessing this information through Python along with a name space that minidom can use for parsing. Using the URLlib library to fetch the RSS feed and a mindom to parse it, the weather sensor can currently query weather info by area code and display this information as text.

An issue to address is the need to map airports to area codes so that weather data can be correlated with flight data.

Yahoo!'s weather service provided an easy and reliable way to gather weather data which is provided with a name space and support for maintaining the code.

Another approach is to obtain weather information around the world from NOAA (National Oceanic and Atmospheric Administration) and the National Weather Service [12]. The world weather information for all airports around the world is based on International Civil Aviation Organization codes.

Current and recent METAR reports are obtained using the NWS anonymous FTP site [13]. METAR observations are available as individual reports or as hourly files. The information available is represented in a meteorological code, however. Extensive information is available about the METAR code and is furnished by the National Environmental Satellite, Data, and Information Service (NESDIS).

Weather information is collected periodically for analys during simulations. A filtering program obtains all of the information required from the METAR reports that are downloaded.

The ftp site for the weather information in NWS is maintained by the U.S. government. Accessing its information is robust and available worldwide.

1.4 U.S.threat Sensor

This sensor reads the current threat level from the Department of Homeland Security website [14] and writes the level and a timestamp to a text file. The program makes a conversion between the word/color system used by the government and a numerical representation for internal use by the DDDAS.

1.5 Data Store

Originally we planned to just make a custom, minimal data store program, perhaps using flat files with an interface suitable for later conversion to a full database. However, after looking at the evolving requirements, we decided to use a SQL database system [15] and eliminate the need to change later. We chose postgres as the database and installed it on our central project server. Like many well behaved open source projects, this one installed from source without significant difficulty.

Two databases where built, travel_dddas_dev and travel_dddas_prd. The dev database is a working area to develop and test sensors, predictors, and correctors without affecting the master data store which lives in prd. When a particular tool is completed and debugged it can then be connected to the _prd database. The _dev database is to be periodically overlaid with the contents of _prd to reseed it with valid data.

Each data table begins with a triplet EPOCH, SENSORID, and DATATYPE, where EPOCH is a timestamp in seconds past the epoch format, SENSORID is a DDDAS-wide unique value typically consisting of the fully qualified hostname plus some arbitrary string, and DATATYPE categorizes the data type by the sensor program that produced it. Taken together these uniquely identify a data point in time and throughout the table space while associating it strongly with its source. After the triplet, domain specific entries for the specific data type fill the rest of the columns in the table row. We standardize the same format for storing all our data, which is extremely useful in cross-referencing interdependent data points such as predictions to weights.

1.5 Transport

The transport module serves as a link between the sensors and the simulation unit. It is based on a Java point-to-point communication tool developed by Wei Li [16]. The original communication tool is not suited for easy deployment on multiple computers. Therefore the software had to be suitably packaged and modified to allow easy installation on many computers. In addition, we use other data transporters such as secure shell copy (scp) and postgres ssl clients. Our DDDAS is designed for flexible data collection and distribution. Fig.3 is a diagram of the data transport system.

1.6 Predictor

In order to decide if a flight will be canceled or seriously delayed, a prediction is made based on information about the weather conditions and U.S. Threat level. To calculate whether or not a flight is going to be delayed the predictor produces a value from 0 to 1, the higher the value the more likely the flight will be delayed. To obtain a value, weather statistics along with the current U.S. terrorist threat levels are used. Weather information currently includes wind speed, wind direction, precipitation type, temperature, and visibility. These factors are also given weights by the corrector from 0 to 1 to judge the significance of each factor in the total outcome.

Each factor is described in detail by introducing fuzzy functions for certain various weather conditions over certain overlapping ranges of input parameters, e.g., very cold (less than -3°C), freezing (-7 to +7°C), normal (+4 to 35°C), hot (above 30°C). The fuzzy functions will be combined by set operations using a T-norm.

In this way the corrector can adjust the prediction to fit the actual outcome. Fig.2 is a diagram of the structure of the system. Once sufficient data has been obtained from flight histories, the values of the individual pieces of data, such as precipitation, can be analyzed alongside whether or not a delay occurred. With this data a polynomial fitting of the data can be used in the calculation of further predictions.

1.7 Corrector

The purpose of the corrector is to compare a previous prediction with the actual results and adjust weights accordingly. If the predicted result is within a certain tolerance, no correction is necessary and the corrector finishes. If the actual result is significantly different from the prediction, the corrector must determine what weights to adjust so that future predictions will be more accurate. Adjustments should use previous data to determine what factor(s) contributed most to the predictor's divergence from the actual result.

While the corrector runs, it finds the last prediction that has corresponding actual results. Once the prediction is found, entries in the airline table are extracted if they match the prediction's flight number and sensor ID. Any of these entries occurring after the prediction's epoch have their results compared to the prediction's result (i.e., the flight was on time, delayed, or canceled). If the prediction was incorrect, we use our prediction's weight epoch key and weight sensor ID key to find the weather conditions corresponding to the time of the prediction. We then query the weather table for similar weather conditions. The airport codes and epoch times for these weather entries are used to query the airline table for flight numbers occurring under similar weather conditions. These flight numbers are then used to query the prediction table to find predictions that were made under similar conditions. The predictions that are correct are compared to the prediction being corrected to mark weather factors that are similar to correct results.

For example, if the prediction was that the flight would be delayed, and it was on time, the corrector looks at the weight epoch key and weight sensor ID key of the prediction. It performs a query on the weather table looking for a match to these two keys. Let us say the result gives airport code LEX, 10 degrees Celsius, Raining, 40% humidity, visibility 10, wind NNE, and wind speed 30 mph. We then query the weather table for any entries with LEX, 5–15 degrees C, Raining, 30%–50% humidity, 5 –15 mile visibility, wind N to NE, and wind speed 20–40 mph. The airport codes and epoch time in the resulting list are then used to query the airline table for flight numbers. Consider queries on flights 116, 314, and 211. The prediction table is then queried for these flight numbers, and the results of these predictions are examined. What if the predictions for 116 and 211 are wrong, but the prediction for 314 is correct. The weather conditions for flight 314 are compared to the weather conditions during our current prediction, and any weather factors that are sufficiently similar are not adjusted. Any weather factors not omitted by the comparison with 314 are examined to see which one changes the most. The weight for this factor from the previous correction table entry for the sensor is then adjusted in the direction of the actual result (on time). The new correction record is then added to the correction table. If no correct past predictions are found for these flights, then a weight is randomly adjusted in the direction of the actual result and a new record is added to the correction table.

2. FUTURE WORK

Flight sensors all suffered from common problems, the lack of a known standard API and regular redesigns of airline web pages. This combination makes keeping a stable suite of flight sensors an ongoing project. We have observed that, if a sensor is well built, changes in the website can be detected and support notified to adjust the page filtering. The time to correct filters is quite low, but still requires manual intervention.

In sharp contrast, weather sensors benefited from the robust and well developed APIs provided by the weather sites utilized.

The present corrector does not adequately adjust factors for national threat level or historical flight data. Improvements are planned for future implementations of both the predictor and corrector. A further improvement to the corrector model is to allow the corrector to set initial weights be finding the best fit for historical data. This process could also be used to reset in the event that predictions do not seem to be improving over time due to poor initial values for the weights or unusual patterns that will take a long time to self correct. Using multiple correctors with different initial weights or different thresholds defining "similar" weather and comparing their results might also yield better performance over time.

3. CONCLUSIONS

We have shown that a system to predict flight timeliness has no technical obstacles. We were successful in collecting data from airline and weather internet sources. We have a method in place to distribute that data, a dedicated database to store the data, and a framework for predicting airline timeliness and correcting predictions over time. We believe that future development of these components would lead to a viable commercial product.

REFERENCES

[1] http://www.dddas.org, Includes project descriptions, many DDDAS workshop virtual proceedings, and links to DDDAS software.

[2] K. Baldridge, G. Biros, A. Chaturvedi, C. C. Douglas, M. Parashar, J. How, J. Saltz, E. Seidel, A. Sussman, January 2006 DDDAS Workshop Report, *National Science Foundation*, 2006, http://www.dddas.org/nsf-workshop-2006/wkshp_report.pdf.

[3] 2003 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science - ICCS 2003: 3rd International Conference*, Melbourne, Australia and St. Petersburg, Russia, June 2-4, 2003, Proceedings, Part IV, P.M.A. Sloot, D. Abramson, A.V. Bogdanov, J.J. Dongarra, A.Y. Zomaya, Y.E. Gorbachev (Eds.), *Lecture Notes in Computer Science*, Vol. 2660, Springer-Verlag Heidelberg, 2003, pp. 279-384.

[4] 2004 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science - ICCS 2004: 4th International Conference*, Kraków, Poland, June 6-9, 2004, Proceedings, Part III, Marian Bubak, Geert Dick van Albada, Peter M. A. Sloot, and J.J. Dongarra (eds.), *Lecture Notes in Computer Science series*, vol. 3038, Springer-Verlag Heidelberg, 2004, pp. 662-834.

[5] 2005 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science - ICCS 2005: 5th International Conference*, Atlanta, Georgia, USA, May 22-25, 2005, Proceedings, Part II, Vaidy S. Sunderam, Geert Dick van Albada, Peter M.A. Sloot, Jack J. Dongarra (eds.), *Lecture Notes in Computer Science series*, vol. 3515, Springer-Verlag Heidelberg, 2005, pp. 610-745.

[6] 2006 Dynamic Data-Driven Application Workshop, F. Darema, ed., in *Computational Science – ICCS 2006: 6th International Conference*, Reading, UK, May 28-31, 2006, Proceedings, Part III, edited by V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, and J.J. Dongarra, *Lecture Notes in Computer Science* 3993.

[7] C. C. Douglas, A. Deshmukh, M. Ball, R. E. Ewing, C. R. Johnson, C. Kesselman, C. Lee, W. Powell, R. Sharpley, "Dynamical data driven application systems: Creating a dynamic and symbiotic coupling of application/simulations with measurements/ experiments," *National Science Foundation*, Arlington, VA, 2000. http://www.dddas.org/nsf-workshop-2000/worksop_report.pdf.

[8] http://www.delta.com.

[9] http://ww.python.org.

[10] http://www.ua2go.com

[11] http://developer.yahoo.com/ weather.

[12] http://nws.noaa.gov/

[13] ftp://tgftp.nws.noaa.gov/data/observations/metar

[14] http://www.dhs.gov/xinfoshare.

[15] http://en.wikipedia.org/wiki/SQL.

[16] Wei Li, "A Dynamic Data-Driven Application System (DDDAS) Tool for Dynamic Reconfigurable Point-to-Point Data Communication," *Master's Thesis*, University of Kentucky, December 2006.

Ray Hyatt, Jr. is a graduate student pursuing an advanced degree in Computer Science. He earned his undergraduate degree in Computer Science from the University of Kentucky in 1996. He has worked professionally as a consultant in high end enterprise wide unix systems administration for over 10 years. His research interests include distributed systems, automation, parallel processing, highly available systems, game theory, and systems administration.

Craig C. Douglas is a professor of computer science and mechanical engineering at the University of Kentucky and a senior research scientist of computer scientist at Yale University. He has also held positions at Duke Univeristy and the IBM Thomas J. Watson Research Center. He will be on sabbaitical at Texas A&M during the 2007-2008 academic year. He has a Ph.D. (1982), M.Phil. (1980), and M.S. (1978) in computer science from Yale University and an A.B. (1977) in mathematics from the University of Chicago.

Divya Bansal, **Soham Chakraborty, Jay Hatcher**, **Chun-Lung Lim**, **Mark Maynard**, and **Trevor Presgrave** are graduate students in computer science at the University of Kentucky.

Gundolf Haase is a professor of mathematics at and computational sciences at the Karl-Franzen University of Graz.

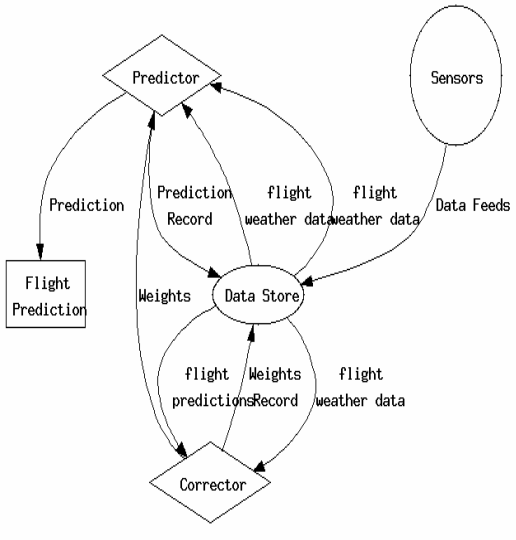


Fig.1. DDDAS Overall Model

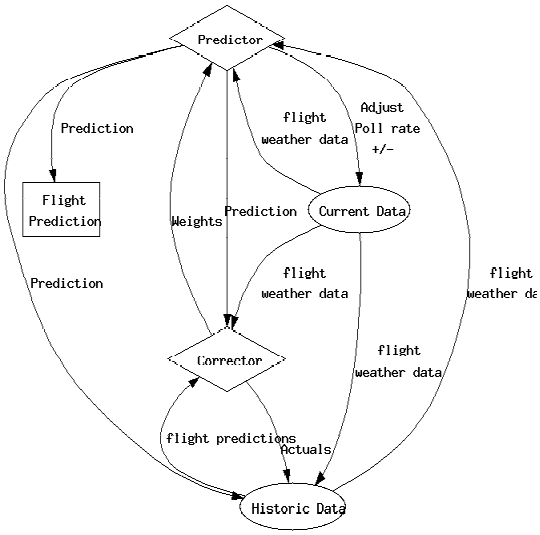


Fig.2. DDDAS Predictor Model

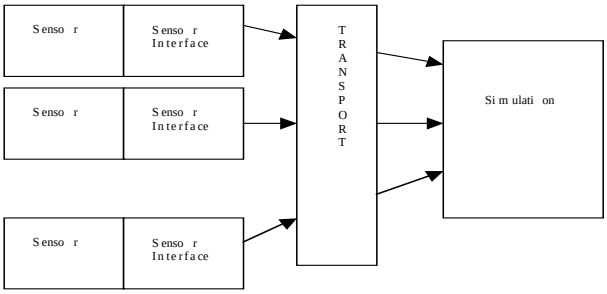


Fig.3. Data Transport System

Parallel Randomized Quasi-Monte Carlo Simulation for Pricing Asian Basket Options*

Daqian Chen [1], Yonghong Hu [2], Qin Liu [3], Xuebin Chi [1]
[1] Super Computing Center, Computer Network Information Center, Chinese Academy of Sciences
Beijing, 100080, China
[2] School of Statistics, Central University of Finance and Economics
Beijing, 100081, China
[3] Guotai Asset Management, Co., Ltd.
Shanghai, 200001, China
Email: dqchen@sccas.cn

ABSTRACT

In practice, no analytical closed form solutions existing can price basket options. In this paper, we present Monte Carlo (MC) simulation on the evaluation of these derivatives. Usually, MC simulation requires too much compute time. This requirement limits most of MC simulation techniques to using supercomputers. By using MPI, our parallel method which combines with the randomized quasi-Monte Carlo technique is implemented on Shenteng 6800 Supercomputer. We perform parallel run time analysis of the proposed method and prove that the parallel approach is scalable.

Keywords: Parallel Computing, Randomized Quasi-Monte Carlo, Black-Scholes Model, Asian Basket Options, Speed-Up, Efficiency

1. INTRODUCTION

As an alternative to Monte Carlo (MC), the quasi-Monte Carlo (QMC) methods refer to a class deterministic numerical technique to approximate integrals in more than 2 dimensions. The idea of QMC methods uses quasi-random sequences instead of (pseudo) random numbers like in MC. These sequences are used to generate a set of points that covers the integration domain very uniformly, so that a better sampling can be achieved.

Recently, the QMC methods become more widely popular in computational finance. Particularly, now, many difficult and complex financial engineering problems, such as valuation of multidimensional options, path-dependent options and interest options can be tackled to obtain approximate solutions by this technique.

The commonly used MC simulation procedure for option pricing can be briefly described as follows: firstly simulate sample paths for the underlying asset price; secondly compute its corresponding option payoff for each sample path; and finally average the simulated payoffs and discount the average to yield the price of an option.

In this paper, we will present some of the issues related to the formulation for pricing Asian basket options using the Black-Scholes model. In the second part,a parallel application of randomized quasi-Monte Carlo for pricing Asian basket call option will be illustrated.

* Supported by 863 program "Environment of super computing service face to scientific research" (2006AA01A116) and National Natural Science Foundation of China "Research on basal Applications of parallel algorithms for present Parallel computer" (60533020).

1.1 The Black-scholes Model

Before going further, let us reduce the formulation for pricing Asian basket options. An Asian basket option is an option whose payoff depends on the average value of the prices of a portfolio (or basket) of assets (stocks) at different dates. Black and Scholes assumed a model for stock price dynamics that is formally described as geometric Brownian motion. This model has the following form:

$$dS=\mu Sdt+\sigma Sdz, t\in[0,T], \quad (1)$$

where the parameters μ and σ are constant with respect the risk free interest rate and the volatility of the asset S, dS is the change in the asset price over the time interval dt, and dz which is the Wiener process for the underlying asset, is drawn from a normal distribution with mean zero and variance dt.

Using Ito's lemma, we then find that the process followed by $G = \ln(S)$ is:

$$dG=(\mu-\sigma^2/2)dt+\sigma dz, \quad (2)$$

where dG is the change in value of $\log(S)$ over the time interval dt, as generalized Wiener process. Let $f(S,t)$ denote the value of any derivative security at time t, when the stock price is $S(t)$. It can also be shown that the value of an option f satisfies the following (Black-Scholes) partial differential equation (PDE):

$$\frac{\partial f}{\partial t}+rS\frac{\partial f}{\partial S}+\frac{1}{2}\sigma^2S^2\frac{\partial^2 f}{\partial S^2}=rf, \quad (3)$$

where r is the risk free interest rate.

The above equations can be generalized to deal with multi-asset options. For example, an option has n underlying assets. We assume that the expect rate of return of all underlying assets is equal to the free-risk interest rate. The model has the following form:

$$dS_i = \mu S_i dt + \sigma S_i dz \quad i = 1, 2, \cdots, n. \quad (4)$$

We assume the usual lognormal diffusion process:

$$dG_i=(\mu-\sigma_i^2/2)dt+\sigma_i dz_i, \ i=1,2,\cdots,n, \quad (5)$$

where i is refers to the value associated with the i th asset. These processes can be correlated between dz_i and dz_j. We can also write the above equation in vector form by introducing the n element vector dG which is normally distributed as:

$$dG\sim N(y,\Sigma), \quad (6)$$

where y is the mean vector, and Σ is the covariance matrix. The elements of the Σ are:

$$\Sigma_{ij} = \begin{cases} \sigma_i^2 & \text{if } i=j \\ \sigma_i \sigma_j \rho_{ij} & \text{if } i \neq j \end{cases}, \quad (7)$$

where $i, j=1,2,\cdots,n$ and ρ_{ij} is the correlation coefficient between the i th asset and the j th asset. The elements of the mean vector y are:

$$y_i = r - {\sigma_i}^2 / 2 \text{ if } i=1,2,\cdots,n . \quad (8)$$

The value f of an option on n assets now satisfies the following PDE:

$$\frac{\partial f}{\partial t} + \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \Sigma_{ij} S_i S_j \frac{\partial^2 f}{\partial S_i \partial S_j} + r \sum_{i=1}^{n} S_i \frac{\partial f}{\partial S_i} = rf . \quad (9)$$

For an Asian basket call option on n assets, m observation times, which payoff at option maturity time (T) is:

$$Payoff = \max[0, \frac{1}{nm} \sum_{i=1}^{n} \sum_{j=1}^{m} S_i(t_j) - X], \quad (10)$$

where $S_i(t_j)$ is the value of the i th asset at the j th time.

1.2 Monte Carlo Simulation

Closed form solutions would be ineffective in determining pricing of basket options as estimating correlations between the underlying assets become problematic in these high-dimensions and hence no analytical closed form solutions exist in practice.

So far, the most effective known method for pricing basket options is MC simulation using a stochastic volatility model and a correlation matrix linking the constituent assets as well as the assets to volatility. Take an Asian basket call option for example, to estimate $\mathrm{E}[f(U)]$, where

$$\mathrm{E}[f(U)] = e^{-rT} \max[0, \frac{1}{nm} \sum_{i=1}^{n} \sum_{j=1}^{m} S_i(t_j) - X] \quad (11)$$

is the net discounted payoff. We suppose that $(S_1(t), S_2(t), \cdots, S_n(t))$ obeys a geometric Brownian motion. Then,

$$f(U) = g(V), \quad (12)$$

where $V=(V_1, V_2, \cdots, V_s) \sim N(0, \Sigma)$ and $s=nm$. To generate V, we can decompose $\Sigma = CC^T$ by applying Cholesky decomposition to release the correlation between different assets, generate random normal variables with mean of 0 and unit variance, $z=(z_1, z_2, \cdots, z_s) \sim N(0, I)$ and return $V=Cz$. Then, we can calculate all the prices of different underlying asset at different time

$$S_i(t_{j+1}) = S_i(t_j) \exp[(r - \sigma_{S_i}^2 / 2)dt + \sigma_{S_i} V_{i+j*n} \sqrt{dt}], \quad (13)$$

2. RANDOMIZED QUASI-MONTE CARLO

With deterministic QMC methods, it is difficult to obtain the reliable error estimate [3], which has motivated the introduction of randomized quasi-Monte Carlo (RQMC). RQMC has a bit of difference from QMC methods. The idea of RQMC is to use a highly uniformly point set (HUPS) to randomize a point set P_n instead of i.i.d, so that: each individual point has the uniform distribution over $[0,1)^s$, where s is the dimension, and P_n is more evenly distributed than a typical set of independent random points.

Then, point sets can be generated by using a deterministic construction yielding n points and randomized appropriately. In briefly, we let v be a uniform random vector in some space n, then choose a randomization function $h: \Omega \times [0,1)^s \to [0,1)^s$ and construct the randomized version $\tilde{P}_n = \{\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n\}$ of P_n, defined by $\tilde{u}_i = h(u_i, v)$.

For more on randomization techniques and standard constructions form QMC methods. The papers (Owen 1998, L' Ecuyer and Lemieux 2002, and Lemieux 2005) are recommended.

3. PARALLEL IMPLEMENTATION

The prices of derivative securities, such as options, are often found analytically by imposing simplifying assumptions. More recently the advent of powerful numerical procedures and computers has made it possible to price more complex and more realistic derivatives.

In this paper, the algorithm for pricing such options with RQMC is described in the following pseudo code:

```
Algorithm:
decompose the correlation matrix with Cholesky
Σ=CC^T
for i = 1 to N do
 generate a s dimensional vector of unit normal random
 values z with RQMC
 transform V = Cz
  for j = 1 to n do
   for k = 1 to m do
    compute the price of the j th underlying asset on
    the k th time S_j(t_k)
   end for
  end for
  average the prices of n underlying assets on the m
  observation times
  calculate the discounted cash flow of the Asian basket
  option payoff_i
end for
average the discounted cash flows over the N
simulations
```

As shown up, the parallel part in this computation is offered obviously in the main simulation-loop since the random variables have to be combined into a multivariate normal vector. Only when the grain size [2] of the computation is very large in each simulation, the parallelism is usable with MPI.

In our case, the RQMC simulation for pricing an Asian basket call option is simple to be parallelized, because there is no correlation among the simulations and no dynamic scheduling. The algorithm runs in parallelism on each processor by computing the option's value for N paths, and only in the end, one processor collects the results from all the other processors without any communication which is very high efficiency during the computing.

4. NUMERICAL TESTS

The goal of parallel computing is generally to speed up the computation. Two important concepts are the *speed-up* defined as $S(x)=t_s/t_p$ where t_s is the serial execution time and t_p is the parallel execution time using x processors; the efficiency $E=t_s/(t_p\times n)=S(n)/n$ is the proportion of the time devoted to performing useful computational work. In best case, the speed up is linear with the number of processors used increasing and the efficiency stays constant and close to 1. When increasing the problem size together with the number of processors, if the efficiency can be kept constant, then the problem is said to be scalable.

The RQMC option price for a given N paths and x processors can be computed according to the above algorithm. And in our case, we use a shifted Korobov lattice [4] deterministic construction yielding point sets and then randomizing appropriately (Lemieux and Jennie La).

The numerical tests were made on Shenteng 6800 Supercomputer under MPI, for the Asian basket call option: the initial price of all underlying assets S=100, the strike price X=100, the risk free interest rate r=0.05, the volatility of all underlying assets $\sigma = 0.2$, the maturity time T=1, the number of the underlying assets n=10, the correlation among assets $\rho = 0.1$, and the number of the observation times m=10. These prices were computed with sample 10^3, 5×10^3, 10^4, 5×10^4, 10^5, 5×10^5, 10^6 paths in order to examine the impact caused by different numbers of sample paths. Table 1 represents the value of the option and the parallel execution time is shown in Table 2.

Table 1 Value of the Asian basket call option

$N \setminus x$	1	2	4	8	16
10^3	3.64299	3.76445	4.03077	4.15533	4.21206
5×10^3	3.72773	3.65706	3.61619	3.5003	3.81949
10^4	3.61636	3.64845	3.7209	3.62664	3.49064
5×10^4	3.73151	3.69555	3.6426	3.67198	3.72048
10^5	3.71274	3.73045	3.7268	3.72016	3.58508
5×10^5	3.70093	3.69255	3.71729	3.71949	3.71981
10^6	3.68907	3.70057	3.69179	3.70384	3.71739

Table 2 Parallel Execution Time

$N \setminus x$	1	2	4	8	16
10^3	0.227983	0.11466	0.058417	0.033293	0.01971
5×10^3	1.36496	0.571115	0.29045	0.148505	0.072359
10^4	2.57798	1.1426	0.58063	0.288986	0.144402
5×10^4	12.3495	5.7128	2.90134	1.44538	0.722973
10^5	25.7394	11.4288	5.7921	2.88568	1.44421
5×10^5	126.054	57.1898	28.9773	14.4267	7.22547
10^6	249.998	114.365	57.9704	28.9125	14.4364

It can be seen that the value of the Asian basket call option converges with the number of sample paths increasing. The serial execution time increases extremely, when the number of sample paths increases, but, at the same time, the parallel execution time decreases when the number of processors increases.

As two measures of the parallel speed-up and the parallel efficiency, which are mentioned above, characterize the quality of the parallel algorithm. Table 3 shows the parallel speed-up and the parallel efficiency, and Fig.1 shows the speed-up by x processors for the 5×10^5 sample paths obtained.

Table 3 $S(x)$ and E for 5×10^5 sample paths

N	2	4	8	16
$S(x)$	2.204134	4.350095	8.737549	17.44579
E	1.102072	1.087524	1.092194	1.090362

The parallel efficiency is constant approximately, when the number of processors is increased accordingly.

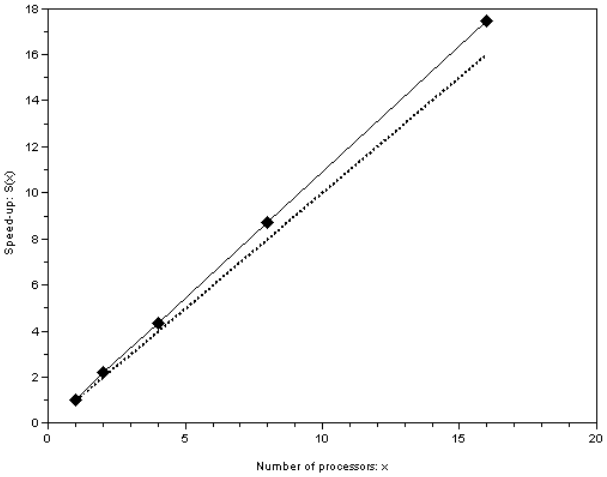


Fig.1. Speed-up for 5×10^5 sample paths

It is observed that $S(x)$ increase linearly with the processors. A constant parallel efficiency can be maintained if the number of processors and the size of the problem are increased accordingly.

5. CONCLUSIONS

Using parallel randomized quasi-Monte Carlo numerical method for pricing Asian basket options is considered. Numerical tests were performed for a number of processors on Shenteng 6800 Supercomputer.

This study describes an application of parallel computing in the finance industry. Options are continuously growing more complex and exotic, and for an increasing number of pricing problems, no analytical solutions exist. Sometimes the speed of pricing options is too slow to accept it. This is where the advantage of parallel computing appears.

Parallel models are required for performing large scale comparisons between model and market prices. Parallel models are useful tools for developing new pricing models and applications of pricing models.

In our parallel implementation we calculated one price of the Asian basket call option. To compute this price by RQMC simulation we need more computational power. Using x processors the execution time is about x times small.

REFERENCES

[1] John C.Hull, *Options, Futures, and Other Derivative Securities*, Huaxia Publishing, 1997.
[2] BarryWilkinson, Michael Allen, *Parallel Programming*, China Machine Press, 2005.
[3] Christiane Lemieux, "Randomized Quasi-Monte Carlo: A Tool for Improving the Efficiency of Simulations in Finance," in *Proceedings of the 2004 Winter Simulation Conference*, 2004.
[4] Christiane Lemieux, Jennie La, "A Study of Variance Reduction Techniques for American Option Pricing," in *Proceedings of the 2005 Winter Simulation Conference*, 2005.
[5] Martin Haugh, "The Monte Carlo Framework, Examples from Finance and Generating Correlated Random Variables," *Monte Carlo Simulation*, 2004.
[6] Pierre L'Ecuyer, "Quasi-Monte Carlo Methods in Finance," in *Proceedings of the 2004 Winter Simulation Conference*, 2004.
[7] P.Pellizzari, Efficient Monte Carlo Pricing of Basket Options, 1998.
[8] John R. Birge, Quasi-Monte Carlo Approaches to Option Pricing.
[9] Hongme Chi, Peter Beerli, Deidre W.Evans, and Micheal Mascagni, On the Scrambled Sobol Sequence, 2005.
[10] Zizhong J. Wang, Huiqing H. Yang, and Jiu Ding, The Study of Quasi-Monte Carlo in the Parallel Computation of Invariant Measures.

Daqian Chen, student in Super Computing Center led by Chi Xuebin at Computer Network Information Center, Chinese Academy of Sciences. His research focuses on parallel computing and its applications.

Yonghong Hu, associate professor, and Director of statistic theoretic department, School of Statistics, Central University of Finance and Economics. His research focuses on financial time series analysis.

Progress on Waterline Classifying Methods & a New Waterline Classifying Algorithm Based on DEM *

Chongliang Sun[1,2] Yunqiang Zhu[1]
[1.] Institute of Geographic Sciences and Natural Resources Research, CAS, Beijing 100101
[2.] Graduate University of the Chinese Academy of Sciences, Beijing 100049
Email:suncl@lreis.ac.cn

ABSTRACT

There exist many points to be improved on the current waterline classifying methods. The singularity of the classifying parameter leads to the lower precision of classifying result, and lack of interknit among the waterlines. On this background, this paper analyzes the progress on the study of valley streamline automatically classified methods, and the progress on Feature-Based GIS theory fully. At the same time the paper concludes the current problems and put up with the idea of designing the classifying algorithm to construct the classifying model based on FBGIS. Particularly, the model will take into account of the natural factors such as the land use and the social factors such as the scale of the city along the waterline, the amount of population of the city & the social-economic condition, etc. At last the paper gives us a discussion of the classifying methods.

Keywords: Classifying Algorithm; Waterline Classifying; FBGIS; Vector Data Structure.

1. THE PROGRESS ON THE WATERLINE AUTO-CLASSIFYING STUDY BASED ON DEM

There exits several waterline auto-classifying methods, among which the popular one are Strahler coding method and Shreve coding method, which are used by the software of ArcGIS. In addition, the Horton coding, Garbrecht coding and the Pfafstetter coding methods are also the auto-classifying methods. In 1945, according to the self-similitude feature of the waterline, Horton put forward his waterline classifying method, which is the Horton coding [1].

(1) Horton coding

The Horton coding indicates the natural result of the water flowing, and it is based on the waterline rank. According to the Horton coding, the waterline can be classified into N grades, and the main waterline would be set to grade(N), and the second one should be set to grade(N-1), and so on. At last, the leaf waterline would be set to the grade(1). There are several characters as following:

1) The Horton coding is a kind of coding method aiming at the geographic waterline entity.
2) The Horton coding reflects the rating relationship between the waterlines. And the Horton code of the waterline is corresponding to the rating relationship of waterline themselves.
3) The Horton code reflects the depth of the child-tree. For example, the child-tree with Horton code (N) has the child-tree with Horton code(N-1). So if they are joined, the waterline with Horton code (N) is the father-tree of the waterline with Horton code(N-1). By this rhythm, the relationship between waterlines can be clear. For example Fig.2.1.

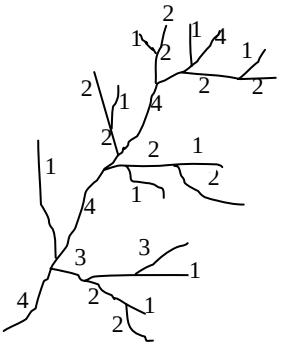


Fig.2.1. The sketch map of Horton coding

(2) Strahler coding

Strahler coding method developed the Horton coding theory. According to the Strahler coding principle, in the ideal waterline, all of the waterlines can be graded into several levels by the nominee principle if they had obvious steady valley. And the leaf waterline with obvious valley would be named the first grade waterline. If two or more than two first grade waterline converge into the second grade waterline, and so on. Anyway, the first grade waterline can flow into not only the second grade waterline but also the third, forth grade or the high grade waterline. Due to this coding method, the series of the waterline reflects not only the grade relationship but the shape difference of hydrological characters[2]. For example fig.2.2.

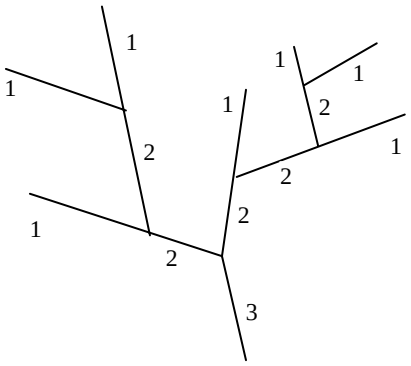


Fig.2.2. the sketch map of Strahler coding

(3) Shreve coding

Shreve coding has it's own principle, that is in the ideal branch-like waterline, all of the troughs with obvious

* This paper is sponsored by the National fundamental scientific platform program—Earth System Science Data Sharing Network(2005DKA32300) .

valley could be graded. The waterline that has no child-tree would be set to the first grade, and two or more than two first grade waterline converge, then it would be the second grade. If two or more than two waterline graded N converge, then it would be the N+1 grade waterline. If a waterline graded N and a waterline graded M converge, at the same time M>N, then the new one would be the waterline graded M, and so on[3]. For example Fig.2.3.

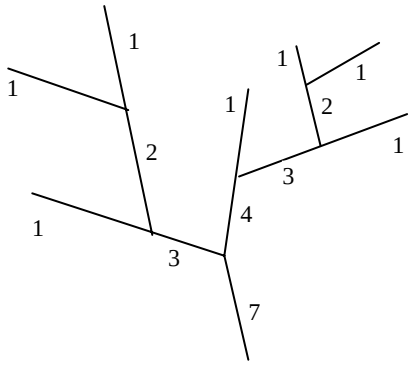


Fig.2.3. the sketch map of Shreve coding

(4) Garbrecht coding
Garbrecht coding was put forward in 1988 by Garbrecht, and it is different from the above coding methods. This method starts coding form the seaport into which the river flow till the end of the river on the left side. After that, it will trace the river in the opposite direction until coming into the new waterline node. On this basis, the waterline would be coded increase by degrees.

(5) Pfafstetter coding
Pfafstetter, a brazilian engineer, recurring to GIS technology, carved up and coded the drainage area with large scale. He extracted waterline form DEM which was modified by him to reduce the error. On this basis, he coded the drainage area with his own methods. And in china, several years later, a researcher mends this method and applies it into the Huanghe river valley.

2. PROBLEMS OF THE CURRENT WATERLINE AUTO-CLASSIFYING METHOD

Although the current auto-classifying methods can code the waterline as a whole in different ways, the classified code under these methods have many problems, the most severe one is the new produced waterline could not match the traditional one. The Horton coding method has less thought of auto-extracted waterline map for it was put forward earlier. Strahler coding method developed Horton coding, but not perfect. And Shreve coding is another new method, not adapt to the traditional waterline. The Pfafstetter coding is near to the practice, and also not perfect. We can judge it form the following:

(1) The current methods lead to the fact that the newly-produced waterline map hardly matches with the traditional waterline map.

(2) During the classifying period, so few parameters were considered, and lack of natural and social factors along the waterline.

(3) The existing methods are lack of the concept of geographic feature, which leads to less relationship between the waterline and other geographic feature, breaking the interlinks among them.

3. STUDY ON THE AUTO-CLASSIFYING ALGORITHM BASED ON FBGIS

3.1 Study on the Feature-based GIS

FBGIS（Feature-Based Geographical Information System）is different form the traditional GIS which is based on the layer. It takes Feature-Based conceptual model and object-based logical model & physical model, with the core of describing and expressing the geographic phenomenon, to recognize and analyze the geographic phenomenon. At the same time, it encapsulates some concrete GIS data structure. Geographic feature has spatial element, thematic element and temporal element. The three parts have the same status in the feature-based model. However, in the layer-based model, the spatial element takes up the dominate status, and this is one of the very important differences between the two models[5]. So the geographic feature includes three-dimension properties, which are spatial properties, thematic properties and temporal properties.

3.2 To Construct the Vector Data Structure Based on the FBGIS

The feature-based GIS data model tends to conceptual modeling stage, and the object-oriented data model can apply to logical model design and the realization of database. To generalize the impersonal world, we should describe it from the following three aspects, that is geometry distribution, thematic element and temporal variety. The geometry information includes the position information and spatial relationship, while the thematic information includes the feature properties and the non-spatial relationship among the features. At the same time, the temporal information describes the transformation of the feature along with time, which can be embedded into the geometry information. The position information of the geometry information can be described by the geometry data model, such as the vector model, etc. And the spatial relation, thematic information and semantic information could be described by the semantic data model. According to this theory, the feature-based waterline vector data structure can be constructed easily, that is to add the topology information and semantic information onto the traditional vector data structure to form it. In the field of spatial information, to improve the shortage of ichnography arc-node data structure in the waterline description, we construct non-ichnography topology and realize it through object-oriented methods. For example Fig.3.1.

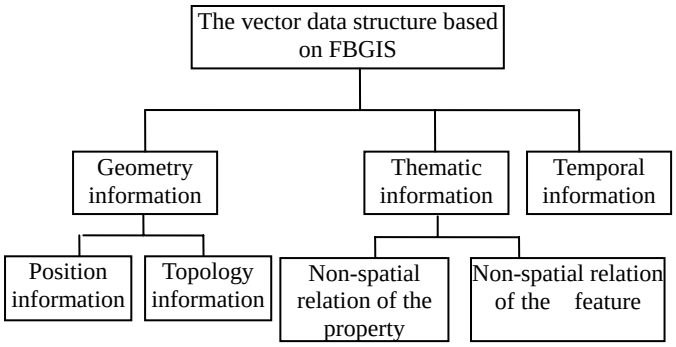


Fig.3.1. The table of constructing the feature-based waterline vector data structure

3.3 The Algorithm of Auto-classifying Model

The majority of the classifying model is to design the auto-classifying algorithm. According to the FBGIS theory, any geographic entity has relationship with the around geographic alternative and this relationship can be described in some certain techniques. During the waterline classifying period, this character could be used fully. At first, the main classifying parameter is the area of certain valleys, by this we can distinguish the waterline grade. If some certain valley area has no obvious difference, the model would grade the waterline by the natural & social factors along the waterline. To deal with the natural & social factors, the suffer analysis could be used based on the FB-vector data structure to establish the data of land use & population of the city along the waterline. And at last the graded waterline data would be produced by this principle.

On the basis of auto-extracted waterline from DEM data, combining with the natural & social factors and the map topology, the waterline auto-classifying model can be established. The detail algorithm is as follows: the model starts trace the waterline from the seaport into which the waterline flows to the direction of upper branches. When come into with the child-branch, the model will make decision which is the main branch till the leaf branch of the waterline, and record it as the main branch setting it the certain ID value. After this, the model would trace the other branches which converge with the main one from the converging node to the upper branch direction till the leaf branch, and so on, then setting it the ID value. And the model will automatically extracts a certain area of a valley to be as an import parameter.

The importing parameters comprise natural & social parameters. And the social parameters include the scale of the city along the river, the number of the population in the city, and the social & economic conditions etc. While the natural parameters include land use along the waterline such as the construction land, agricultural land, forest land, unused land, as well as the runoff of the river. The weight of every parameter would accord to the practice. For example Fig.3.2.

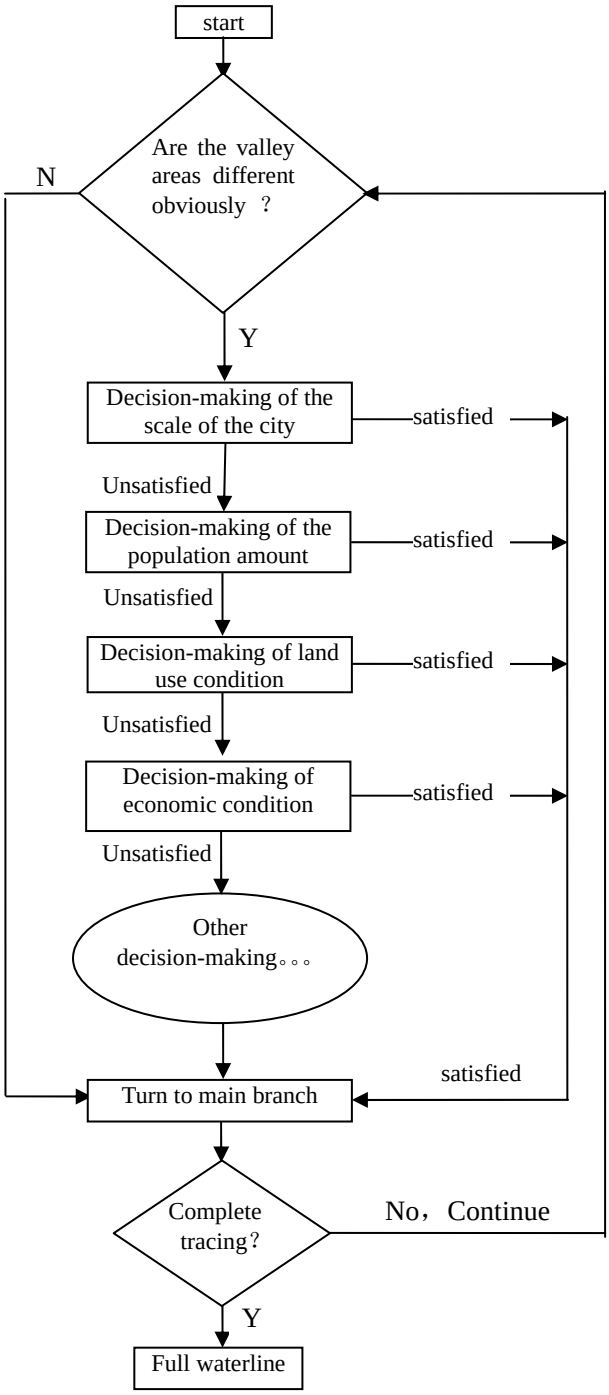


Fig.3.2. Figure of the classifying algorithm of the model

4. DISCUSSION

This paper concludes the progress of the waterline auto-classifying methods and analyzes the existing problems of the auto-classifying method. And the paper puts forward a new classifying method based on the FBGIS under the background of practical use, which had been applied into practice. The author take for that this method would represent the direction of the waterline classifying study for it's produced data has obvious geographic feature and is close to the natural things.

REFERENCES

[1] Luo Wenfeng, Li Houqiang,etc. “Horton law and the description of branch network”[J], Progress on the water sciences. 1998. 9(2):118-123. (In Chinese)

[2] Zhao Chunyan. “Integrated study of Horton code & graphics of the waterline” [D]. Master paper of University of Wuhan. Wuhan. 2004. (In Chinese)

[3] Xu Baorong, Yang Taibao. “The analysis of affluence on simulation of waterline network in the arid area based on DEM” [J]. Transaction of University of Lanzhou （Natural Science Edition）. 2006. 42(1):27-32. (In Chinese)

[4] Luo Xiangyu, Jia Yangwen, *et al*. “The coding method of waterline based on DEM & practical survey network” [J]. Progress on the water sciences. 2006. 17(2):259-264. (In Chinese)

[5] Zhou Chenghu, Lu Feng, Qing Wan. “A conceptual model for a feature-based virtual network” [J]. Geoinformatica, 2000, 4(3):271~286.

Chongliang Sun, is now reading for PH.D. with the major of GIS in the Institute of Geographic Sciences & Natural Resources Research, CAS. And his interest is focused on the application of GIS/RS, especially on the study of DEM theory & application. And he also made some important task on the waterline auto-extract and auto-classified research.

Yunqiang Zhu is an Assistant Researcher of Institute of Geographic Sciences and Natural Resources Research, CAS (Chinese Academy of Sciences). He received his Ph.D degree from CAS in 2006. His main research interests include GIS development, 3S application in land and water resources management, and Geo-data sharing which involves multi-data integration, data sharing policy and standards, network platform development, etc.

Study on Complex Products Collaborative Design for Assembly under Distributed Environment

Shijing Wu, Mingxing Deng, Jing Xie, Lilun Luo
School of Power and Mechanical Engineering, Wuhan University
Wuhan, Hubei, China
Email: ycdmx@126.com

ABSTRACT

Considering all the factors that affect the assembly performance of a product, design concept and contents of collaborative design for assembly are discussed; model of complex products collaborative design system for assembly under distributed environment is presented, and its function structure model and running mechanism are described from system realization viewpoint. With resources of the whole net, structure detailed design, static structure feasibility analysis and process assembly feasibility analysis are carried out by means of combination of human-computer and human-human collaboration. Finally, system of complex products collaborative design for assembly under distributed environment is realized based on this model.

Keywords: Distributed Environment, Design for Assembly (DFA), Complex Product, Top-Down, Preassembly

1. INTRODUCTION

Complex products design is a kind of design whose composition, technology, design process and project management is complex. The concrete manifestations are as follows: 1) system composition is complex, often being a synthesis of subsystems in different fields; 2) design process is complex, including not only asynchronous design sub-tasks on time axe, but also synchronous design sub-tasks at a time; 3) system's performance is complex as global discussion is needed because that demands of the overall performance is always higher than the demand of a function module. Complex products design process is an integrative collaborative design process in different fields, and also a collaborative design process completed and cooperated by many designers[1]. Complex products' collaborative design demands that all designs must make an organic whole by assembly and simulation, in order to ensure the reliability of the design of every part.

Taking the above facts into consideration, this paper constructs a design model of complex products design for assembly under distributed environment. Based on the Top-Down design method, structure detailed design, static structure feasibility analysis and dynamic process assembly feasibility analysis are carried out by means of combination of human-computer collaboration and human-human collaboration.

2. DESIGN CONCEPT AND CONTENTS

Collaborative design for assembly is a general design method that is the combination of collaborative design and DFA, with people who do works related to design joining in. Based on the digital model, it improves the quality of DFA on the network platform by both collaborative preassembly and assembly ability testing from static structure and dynamic assembly process. The collaborative DFA is an important part of the collaborative design, which plies collaborative structure preassembly and process preassembly to obtain a proper product assembly model and scheme, centering products assembly ability. In this paper, complex products collaborative DFA is studied as follows.

2.1 Top-Down Products Design

The current CAD systems can support Bottom-Up design process that is to complete product assembly design applying geometry constraint after components' detailed design[2]. But Bottom-Up design method could not meet demands of Concurrent Design. In contrast, Top-Down[3] design method starts from functional modeling of product. It completes detailed design of components based on determination of the preliminary product composition and shape, and definition of components' assembly and mutual constraint relations, according to product's functional demands and design constraint. During products design process, assembly constraint determined in the former assembly level would be the design constraint in the next level. This kind of constraint relations should be recorded with the final model to ensure that in subsequent design process and redesign process the system can automatically transfer and meet those constraint relations, for the sake of ensuring the uniformity of product model. Top-Down design method is to design on assembly level, not only on part level, and supports Concurrent Design for complex products. Based on Top-Down product design method, the design task can be divided into many sub-tasks and assembly model could be obtained depending on the constraint determined at the beginning of the design.

2.2 Digital Preassembly

In order to express and demonstrate the 3D digital product model, every component needs to be assembled making use of the assembly function of CAD system. 3D digital preassembly [3]technology is mainly used in the analysis of structure feasibility. It is able to coordinate product structure design, system design and examination of components' location, as well as to reduce redesign and modification, based on 3D modeling of components, management of product data and sharing of design. In the design process of complex products, structure feasibility considers design conflict from the static viewpoint, carrying through static interference detection after obtaining product assembly model from structure preassembly, in order to ensure that there is no conflict in spatial location for components in the condition that they meet all the constraints. So it will find and resolve interference problems on a higher level. This process often follows several steps: (1) call the 3D digital model of product; (2) carry through digital assembly according to constraint condition; (3) detect interference and other incoordination; (4) inform related designers to resolve; (5) call new model for digital assembly, looping till no any interference and incoordination problems; (6) send model information for downstream design.

2.3 Process Assembly Planning

The assembly function of current CAD system can only simply accumulate components---no matter whether there exists any path to assemble, once geometry constraints are defined, components will be located directly. In fact, during physical assembly, components will be influenced by those components that have been assembled already[2]. So, products feasible in structure not always have process assembly feasibility. In order to ensure design's rationality in advance, process assembly feasibility means to discover probable conflict in the assembly process. It is carried out utilizing dynamic preassembly based on the assembly sequence and route constructed by assembly planning. Assembly feasibility, concurrency of operation and assembly cost should be synthetically considered in assembly sequence planning algorithm. This process generally follows the following steps: (1) call upstream non-interferential assembly model; (2) extract model information, plan assembly sequence by applying a large-scale, highly constrained combinatorial optimization algorithm (e.g. ant colony algorithm); (3) if there is no feasible assembly sequence, inform related designers to resolve; (4) call new non-interferential assembly model to plan assembly sequence till find feasible assembly sequence; (5) send model information.

Collaborative design takes advantage of general assembly designers' knowledge and experience of assembly design. The main purpose of collaborative design for assembly is to realize consistent and corporate decision-making bringing the evaluation and proof of product structure feasibility and product process assembly feasibility forward to adjust design in time. Thus, design quality can be raised and product development cycle time can be reduced.

3. COLLABORATIVE DESIGN MECHANISM

3.1 Collaborative Design Process

For complex products design, the general way is to divide product design task into a series of sub-tasks, and then assign them to suitable Task Design Unit (TDU) to accomplish; then the design result is sent to start up the downstream design. Every collaborative designer can do distributed concurrent independent work as well as synchronous negotiation and discuss. Top-Down design method is applied to complex products design. Firstly, function model is built according to product function demands and translated into structure model to complete initial design plan and structure sketch; then product design model driven by constraint is constructed, and design scheme that meets the function demands can be obtained by constraint solving. Product design task is divided into some sub-tasks based on function/structure model. Those sub-tasks, design objection and related parameter are sent to suitable Task Design Unit.

1) Task Design Units (TDUs)
   Design sub-task of TDU is carried out by suitable and experienced designers in this field. Depending on initial product demand analysis/conceptual design and structural design, designers of each distributed Task Design Unit organize design resources and work on their part of the product using their own particular ways to complete their respective design sub-tasks, according to the parameter and design objection sent by sever. Relations among those TDUs are both independent and interactional: design sub-task of which each TDU takes charge of is independent in function or structure; but on the other hand, there are coupling relations among those TDUs, which means that some design variable of one TDU must satisfy constraints in some other TDUs.
2) Static interference detection
   Purpose of static interference detection is to analyze structure feasibility. In current study, interference detection algorithm could be roughly divided into two types: space decomposition approach[6-8] and bounding box[9-11]. The idea behind bounding box is to approximate the object with a simpler bounding box that is a little bigger than the object. In this system model, an assembly-oriented multi-layer exact interference detection algorithm mentioned in literature[12] is introduced. It provides an effective method to resolve the intrinsic time complexity in interference detection. In building different interference detection layer, it speeds up interference detection by pruning away primitive pairs, which will not intersect clearly though rapid intersection test in former detection and just deal with those interferential in the former layer interference detection.
   If there is no static interference, it indicates that the product structure is feasible, and the next assembly feasibility analysis could be carried out by assembly sequence planning and simulation; otherwise, inform related TDUs to modify the design based on negotiation. The next assembly sequence planning and simulation are based on the feasible model obtained in this stage.
3) Assembly sequence planning
   Assembly sequence planning (ASP) is an important research topic in DFA. Many researchers made their research in the assembly planning problem on the basis of De Fazioand Whitney's[13] liaison graph. In particular, methods concerned expert systems[14,15], simulated annealing[16], Petri nets[17,18], neural networks[19,20], genetic algorithms[21,22] and ant colony algorithm[23] have been given more and more attention.

For complex products, the number of possible assembly sequences may be too large to be handled efficiently with traditional methods. In fact, this is a NP-hard problem, so heuristic algorithms are frequently applied. An ant colony optimization strategy is introduced in this paper. Ant colony algorithm is a large-scale, highly constrained combinatorial optimization algorithm. It can generate the optimal assembly sequence because it considers many factors that affect assembly, such as assembly feasibility, parallel operation and assembly cost. In the algorithm of this paper, precedence relations among components are introduced to the searching algorithm; dynamical candidates set strategy based on precedence relations is adopted to constrain the search space of assembly sequence; penalty mechanism is used to help ants avoid the unfeasible sequence; state transition rule and local-global updating rule are defined to ensure acquiring of the optimal solutions.

If there is no feasible assembly sequence, inform related designers to modify the design; otherwise, it shows that the design result is feasible. Flow chart of design is shown in Fig.1.

3.2 Conflict Resolution

Collaboration between different TDUs in complex products design involves both synchronous and asynchronous communication. It involves the ability of the different TDUs to work on their part of the project using their own particular ways yet being able to communicate with the other TDUs to bring about a common objective, the design of the product. Because of mutual influence between different design sub-tasks, conflict is difficult to avoid. Conflict is the essential phenomenon of collaborative design, and its resolution is the

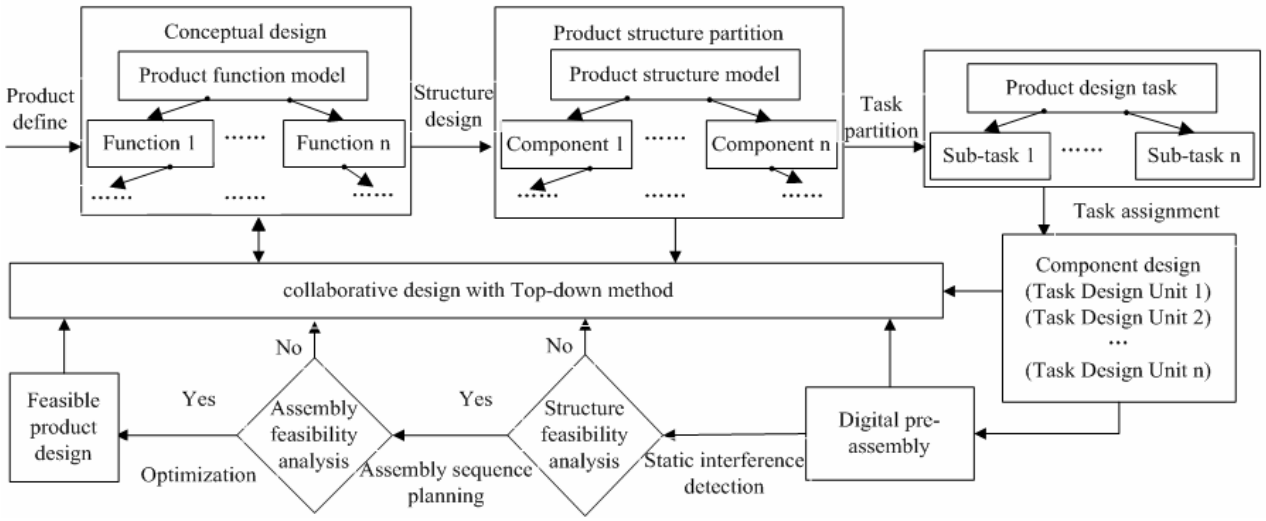


Fig.1. Flow chart of collaborative DFA

process of global optimization of the design. How to resolve conflicts to achieve design coherence is a crucial problem for collaborative design. Conflicts are resolved by combination of rule and negotiation in this paper. Key parameters of model in those interdependent design sub-tasks form a key parameters set, and are managed unifiedly on the server. All the parameters are also associated with their weight coefficient in different TDUs. In 3D digital modeling process, design variables that related to key parameters are restricted with the key parameters, and value of those parameters are set and sent by the server. When conflict happens, one TDU on the client can change a parameter's value only when weight coefficient of the parameter in this TDU is the highest; when the other TDUs need to change the value, it must negotiate with the TDU in which the parameter's weight coefficient is the highest, and if that TDU agrees, the value could be changed, otherwise, it should be resolved concertedly by the server.

4. SYSTEM REALIZATION

This system model is realized by C# and SQL Server2000. C# is a new programming language designed for building a wide range of enterprise applications that run on the .NET Framework. An evolution of Microsoft C and Microsoft C++, C# is simple, modern, type safe, and object oriented. It has excellent function for distributed calculation. The 3D digital model is constructed on the CATIA platform, model information extraction and modification are carried out by CAA（Component Application Architecture）. CAA is the product expansion of Dassault Systems and the power tool of secondary development for clients. CAA can deal with the secondary development work simple or complex and it can integrate with the original system closely. It is very convenient for clients to use. The function of CAA is realized by Rapid Application Development Environment (RADE) and Application Programming Interface (API)[24].

Collaborative design system in this paper runs based on Intranet. By comprehensive use of resources of the whole Intranet, structure's detailed design and assembly ability analysis are solved in the way of human-computer collaboration and human-human collaboration. The mainly framework of the system is shown in Fig.2.

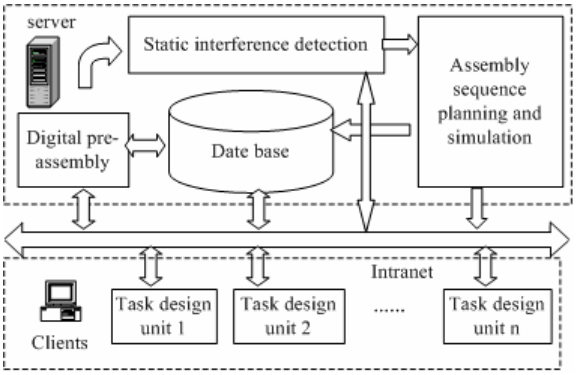


Fig.2. System framework

The system includes one server and ten clients. Based on this system, many designs of complex products are carried out successfully by many design groups under distributed environment, and that shows the system model is efficient.

5. CONCLUSIONS

With the increase of product's complexity and formation of network manufacture mode, study on assembly design technologies and platforms in a new mode become a hot topic in related fields. In this paper, approach of complex products collaborative design for assembly under distributed environment is studied based on research of key technologies of DFA, such as design method, structure feasibility and process assembly feasibility analysis. Then system model for complex products collaborative design is constructed on the Intranet, having many characteristic as follows: 1)supporting human-human collaboration, which means complex products collaborative design could be completed by multi design groups under distributed environment; 2) achieving human-computer collaboration by taking advantages of both traditional CAD system and intelligent optimization algorithm; 3) optimization of products structure & process assembly---optimizing components design in means of negotiation of TDUs and product process assembly utilizing intelligent assembly sequence planning. This system model provides a feasible way for design, communication and decision-making with multi-designers under distributed environment.

Realization of multi-disciplinary and multi-fields collaborative

design on the Internet under distributed environment would be the emphasis in future works, in sake of economizing design cost and improve the overall performance of multi-fields complex products.

REFERENCES

[1] LI Bo-hu, CHAI Xu-dong, ZHU Wen-hai, "Supporting Environment Technology for Collaborative Manufacturing of Complex Product," *Computer Integrated Manufacturing Systems*, Aug.2003,Vol.9No.8, 691-697

[2] Xu Luning, Zhang Heming, Zhang Yongkang, "Research on the key problems in multi disciplinary cooperative design of complex products," *Modern Manufacturing Engineering* 2005(1)10, 10-13

[3] JIANG Hua, XIONG Guang-leng, ZENG Qing-liang, "METHODOLOGY AND TECHNOLOGY OF DESIGN FOR ASSEMBLY," *Computer Integrated Manufacturing Systems -CIMS*, Aug.,1999 Vol.5,No.4,56-60

[4] Tomiyama T, Yoshikawa H, "Extended General Desig Theory[C]," in *Proceedings of the IFIP WG5.2 Workin Conference on Design Theory for CAD*. Amesterdam: Elsevier Science Publishers BV, 1985:95O130.

[5] Wei Yinmei, WU Yuanquan, Shi Jiaoying, "Collision Detection Methods for Virtual Environment [J]," *Computer Engineering & Science*, 2001, 23（2）: 44-47.

[6] M Held, J T Klosowski, J S B Mitchell. Evaluation of collision detection methods for virtual reality fly-throughs [A]. Proceedings of 7th Canada Conference Computer Geometry[C]. 1995: 205-210.

[7] Deng Wen-ping, Xiong Yue-shan, Li Si-kun, "A Fast Algorithm for Collision Detection Based on Bounding Volume Hierarchies of Octree [J]," *Journal of System Simulation*, 2003, 15(S): 158-160.

[8] B Naylor, J A Amatodes, W Thibault, "Merging BSP trees yields polyhedral set operations [A]," in *Proceedings of SIGGRAPH '90[C]*. 115-124.

[9] Zachmann G, " Real-time and exact collision detection for interactive virtual prototyping [A]," in *Proceedings of DETC'97[C]*. 1-10.

[10] Gottschalk S, Lin M C, Manocha D, "OBB-Tree: A Hierarchical Structure for Rapid Interference Detection[A]," in *Proceedings of SIGGRAPH '96[C]*. 171-180.

[11] Wei Ying-mei, "Research on Collision Detection in Virtual Environment," paper for doctor degree.2000.10

[12] LIU Jian-hua, YAO Jun, NING Ru-xin, "Research and Realization of Collision Detection Algorithm in Virtual Assembly Environment," *JOURNAL OF SYSTEM SIMULATION*, Vol. Aug. 2004,16 No. 8,1775-1778

[13] De Fazio, T. L., & Whitney, D. E. (1987), "Simplified generation of all mechanical assembly sequence," *IEEE Journal of Robotics and Automations*, 3(6), 640–658

[14] Choi, C.K., Zha, X.F., Ng, T.L. and Lau, W.S.(1998), "On the automatic generation of product assembly sequences," *Int. Journal of Production Research*, Vol. 36., No.3, pp. 617-633

[15] Zha, X.F., Lim, S.Y.E. and Fok, S.C. (1999), "Development of expert system for concurrent product design and planning for assembly," *Int. Journal of Advanced Manufacturing Technology*, Vol. 15.,No.3, pp. 153-162

[16] Milner, J.M., Graves, S.C. and Whitney, D.E., (1994), "Using simulated annealing to select least cost assembly sequences," *IEEE Int. Conf. on Robotics & Automation*, San Diego, CA, May 8-13,pp: 2058-2062

[17] Thomas, J.P., Nissanke, N. and Baker, K.D. (1996), "Hierarchical Petri net framework for the representation and analysis of assembly," *IEEE Trans. on Robotics and Automation*, Vol.12, No.2, pp. 268-279

[18] Inaba, A., Fujiwara, F., Suzuki, T. and Okuma, S. (1998), "Timed Petri net based scheduling for mechanical assembly – integration of planning and scheduling," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science*,Vol. E-81A., No.4, pp. 615-625

[19] Chen, C.L., (1991), "Automatic assembly sequences generation by pattern matching," *IEEE Trans. On Systems Man. and Cybernetics*, Vol. 21 n. 2, pp: 376-389

[20] Hong, D.S. and Cho, H.S., (1995), "Neural-network based computational scheme for generating optimized robotic assembly sequences," *Engineering Applications of AI*, Vol. 8 n. 2. pp: 129-145

[21] Dini, G., Failli, F., Lazzerini, B. and Marcelloni, F.,(1999), "Generation of optimized assembly sequences using genetic algorithms," *Annals of the CIRP*,Vol.48, no.1, pp: 17:20

[22] Romeo M. Marian, Lee H.S. Luong, Kazem Abhary, "A genetic algorithm for the optimisation of assembly sequences," *Computers & Industrial Engineering* 50 (2006) 503–527

[23] F. Failli, G. Dini, "ANT COLONY SYSTEMS IN ASSEMBLY PLANNING: A NEW APPROACH TO SEQUENCE DETECTION AND OPTIMIZATION, "in *Proceedings of the2nd CIRP International Seminar on Intelligent Computation in Manufacturing Engineering*, 227–232

[24] Cao Chunsheng, "Research on Information Model in Virtual Assembly of Aircraft Structures Based on CATIA/CAA," Nanjing University of Aeronautics and Astronautics, paper for master degree.

Shijing Wu, doctor, professor, Vice dean of School of Power and Mechanical Engineering , Wuhan University. He graduated from Wuhan University of Hydraulic and Electric Engineering in 1983, and got his Master Degree in 1986 in the same University. In 2000, he got Doctor Degree from Wuhan University. His current research interests include structure dynamic performance test & analysis and modern machinery design theory & methods. In recent years, he has done much successful research in large-scale complex engineering machines' structure optimization design and complex mechanical system vibration theory, and completed many significant projects.

Mingxing Deng, Female, doctor candidate. Graduated from the department of Vehicle Engineering in Hubei Automotive Industrial Institute in 2003 and got her Bachelors Degree, then studied in the department of Mechanical Design in School of Power and Mechanical Engineering, Wuhan University, and got a Master Degree in 2005. Since then, she is in School of Power and Mechanical Engineering, Wuhan University as a doctor candidate.

Design and Application of Telephone Auto-payment System

Junhong Zhang [1,2], Ping Zhu [1,3]
[1]School of Computer, Wuhan University, Wuhan, 430072, China
[2]Wuhan branch Hubei Co.Ltd. ChinaTelecom Group, Wuhan, 430071, China
[3]School of Information,Zhongnan University of Economics and Law,Wuhan,430062,China
Email: zhangjh@public.wh.hb.cn

ABSTRACT

In this paper, a new system project for the interconnections between the fixed telecom corporation and banks has been designed, which would help the fixed telecom corporation solve the problem in developing telephone auto-payment business from now. A new auto-payment business architecture and multi-layers application architecture as IN(intelligent network) mode are adapted ,and the coincidence & security management for the payment of the telecommunication services are realized in this project As a new added service, the telephone auto payment is also in practice. All off these would widely enlarge the foreground of application in e-commerce services.

Keywords: Telephone Auto-payment, Architecture, Value-added Services, E-commerce

1. INTRODUCTION

The style of competition in telecom market is changing from struggleing for resources of network to supporting in the fields of businesses and services. How to get best to expand basic business in variouse way, to innovate increment business, and to find new increasing-point of profit is the theme which is thought by all telecom corporations.

Aim to get ahead in the market.,almost every telecom corporations made cooperation with various banks Banks become the new way, on whichtelecom corporations develop their business. With their nature advantage in mobile phone payment, China Mobile Cor., China Unicom Cor. increased their investment on system construction in 2004, and fetch “wallet of Mobile phone”, “As wish 133” prepay business, etc[1]. China Telecom Co. is actively exploring the new way of auto-payment with fixed telephone and PHS (personal handyphone system), especially with the nice trend on PHS business. They hope using their network resources more efficiently, engaging their twice-exploitation in the market of telephone to improve their benefit and to keep the economic increasing.

We will discuss the problems in the points of telephone auto-payment system design and application foreground.

2. BACKGROUND

Now,building the connection between the telecom. Corporation and the banks is a simple thing. Connected with private lines,the business between them are simple,too. There is an only interface getting with the telecom billing system and taking on some simple interconnecting business.

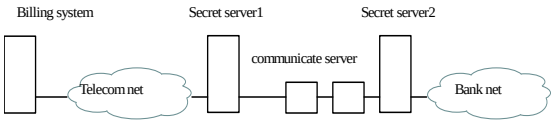


Fig.1. The actual connection between Telecom and Bank

Company with the extended business between the Telecom. and the Bank, some problems will show out.. Such as the system is unable to support more and more Telecommunication services; unable to support the requirement of the trade security etc.

So, we need surely to build new application architecture and standardize the data interface. Making use of the phone and platform of blance resources both from the Telecom and the Banks , We can make a kind of electric payment—phone model which is a new value-added telecommunication services–telephone auto-payment service.We also have done some researchment in the technology realization.

3. DESIGN OF THE TELEPHONE AUTO-PAYMENT SYSTEM

On the new design of our telecom. auto-payment platform ,we completely think about the demand of the business realization in future At the internal interface ,it is able to connect with the billing system, the integrated business support system,10000-number service system, the telecom Intelligent network(IN) platform,etc. It takes on the job to extend and makeup the function for the internal business supporting systems of the telecom corporation. At the external interface, it can connect with the partner banks. It also can connect with the agreement business partners and the custmors[2,3]. The graph of the connection in various platforms as follows:

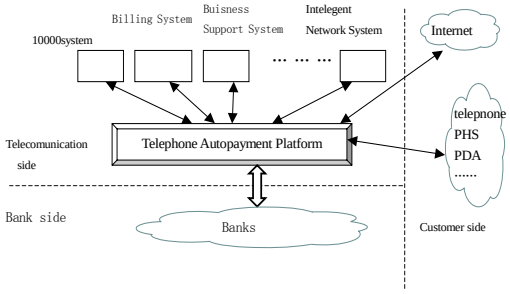


Fig.2. The connection between telephone auto-payment platform and other platforms

3.1 The Components of the Platform

The primary components are DataBase Servers,Web Servers,Communication Servers, network equipments and security equipments. The whole system is designed and constructed assurely to keep the dependability on telecommunication level. The redundant mechanism is adopted in those key equipments. So we can assure the

system run uninterruptedly in 7x24 hours.

Database server：Applying the dealing data management, log management. Either a PC server or a small computer is able to take on the work.Two node should be considered for the security.

Web server：Realizing the Internet connection, applying the query for all the information. PC server is able to take on the work.

Communicating Servers：At least two servers need to set. One for the outside communication with the bank or other application system. One for the inside communication with the telecom. systems such as the billing system,the IN system ,etc. PC server is able to take on the work,too.

3.2 Telephone Auto-payment Business Architecture

There are some original ideas of us in the auto-payment business architecture. We nearly solve the problem that the banks do not participate in this kind of business, such as "mobile phone wallet"[4,5]. We cannot offer the fulfil services without the banks participating in.

At prensent, the auto-payment business mode of telecom corporations is as follows:

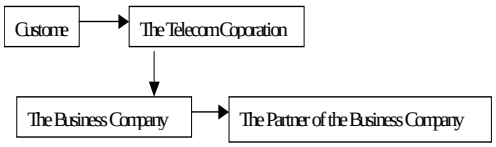


Fig.3. The auto-payment business mode now

The financing flow between the business company and the telecom corporation is: customers➔the telecom corporation➔the business company➔The partner of the business company.

The above flow is doable in technology. Every participator can get more profit if the banks do not participate in this kind of business. But, there are some financial risks existing. In our new business architecture, we take participators from banks into account. The telecom corporation should cooperate with banks if they want to intervent electric payment services[6,7]. We should rebuild the auto-payment value chain. The new chain would be:

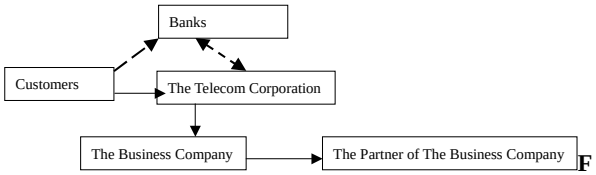


Fig.4. The new auto-payment business mode

The financing flow between the business company and the telecom corporation is: customers➔(banks➔)the telecom corporation➔the business company➔The partner of the business companys.

In the new value chain, the telecom. corporation get the communication fee and some resource rent fee. Banks get bankroll,added-value of the account and some handling charge.

To implement the new payment mode, we have to optimize the resource usage between the telecom corporation and banks in reason. That is why we should divide the jobs in their information tech platforms. It is important to depress the to much cost which banks may burdenmay in the auto-payment business. It has been considered deeply in our project. We setup virtual branch account at our telephone auto-payment platform. The main business process is completed by the telephone auto-payment platform, which can reduce the load of banks' host computers, reduce the load of communication on the network, etc. So all the system cost is depressed.

3.3 Layered Design of the Application Architecture

The application architecture obeyes the all rules of the telecom operation supporting system frame. In the system, every section about technology, operation and architecture can support modularization, expansibility and loose-coupling. Also, the idea of the telecom IN (intelligent network) is adopted. The system is designed to be divided into three layers: shared business connected layer, independent function supporting layer and independent resource supporting layer [8].

business connected layer: It supplies the means and equipments for business connection. Such as E1, ISDN, No.1 signal, No. 7 signal and voice resources,etc. A lot of connecting means give the system strong ability to makeup a network. It can connect with public network and private network. It can connect with fixed telephone network, short message system , Internet,etc. So richful and colorful business are able to be realized in the system.

function supported layer: The business function.would be realized on it. which is logically layer between business connected layer and resource supported layer. It explain the business flow from business connected layer. It also schedule and manage all the resources of this system , the banks' systems and others. It is able to supply some value-added services supporting environment.

resource supported layer: It supply plenty function modules for choosing the resources of outside data resources,inside data resources and business functions resources. The resource distribution strategy are designed. We can expand and optimize the resources conveniently.

The three-layer architecture show the layered system designing idea. Between the layers,the standard protocol or the API enveloped mode are adopted. Every layer has relative independence. Shared business connected layer and independent function supported layer build the business process platform for the telephone auto-payment system. They have the characteristics of business-independent, stabilization, security and standard. The resource supported layer has the characteristics of expandability, optimizability.

3.4 Standard Design of the Communication Interface

To realize the auto-payment business,the platform may have interface with many outside and inside systems or communication equipments,.such as fix telephone,mobile,PDA ,etc. The uniform message format is strictly designed and followed. This can shield the defierence of the connecting systems or equipments. reduce the work for the program coding,testing and maintancing. The socket mode is adopted in the platform. It is decribed as follows:

(1) Packet head control message:

```
struct PktCtlMsg
{
   unsigned long   dwLen;        // length of the packet
   unsigned char   byFactory;    // factory code
   unsigned char    byProgID;    // process ID
   unsigned char byMorePkt;
   char     pCMD[10];
   long     dwStartNum;
   long     dwEndNum;
   long     dwRequestID;
   long     dwAnswerID;
   long    dwSeq;
   char    pRecSep[5];
   char    pFieldSep[5];
   long    dwReserved1;
   long    dwReserved2 ;
};
```

(2) packet body structure

```
  struct PktMsg
  {
  struct    PktCtlMsg    CtlMsg;    // Packet control
  message
short   errorcode;              //0：success, others: fail
char    datatrans[1];           //transfer data
  };
```

4. APPLICATION FOREGROUND

The telephone auto-payment platform is based on the designing idea which is cross-vocation cooperation and resource integration. It is predictable that the platform can mainly achieve tow goals after the platform combined different telecom operation support system with the credit card system.

(1) The basic telecom services change to E-buisness mode. It would satisfy with the requirement of developing telecom business by fully use every channel resources, and consummate bank charging act as an agent for the fixed telecom corporation. Only with a credit card, the customer can enjoy the different services supplied by the telecom corporation like local call, long distance call, IP phone, online, fee, recharge etc. It can also realize short financial messages releasing for PHS, E-phone.

(2) It can exert the advantage of mobile calling of PHS and oper address information of fixed telephones owned by fixed telecom corporations. Phone charging with bundled bankcard would be true. Customers can make real time consumption and payment by select productions with dealing the corresponding phone number. In the beginning it will mainly supply

Auto-payment with deferent game points, even B2B (business to business) mode as productions distribution like cigarette and drinking,etc.

5. CONCLUSIONS

The telephone auto-payment platform would be the most important expanding operation and service means of telecom corporations. Telecom corporations can directly share the resources belong to banks like shop points, customers, human and technology. It would change the basic telecom businesses to E-buisness mode, explore application foreground more widely to phone-business and electronic-business.

REFERENCES

[1] “The component analysis of the mobile paument value chain, Li Dingchuan,” *CHINA Telecom Network* 2005 3

[2] *Network payment and account settle*, Ke Xinsheng, Electronic industry publishing house 2004 3

[3] Electronic Payment Schemes. P. M. Hallam-Baker. http: //www.w3.org/ pub/WWW/ Payments /roadmap.html

[4] Xiaoling Dai,Jhhn Grundy , Bruce W N Lo ,”Comparing and constrasting micro-payment models for E-commerce systems,” icii2001

[5] O’mahony D Tewari, *Electrionic payment systems for E-commerce Boston*:Artech House H 2003//P

[6] Zhao Ying,Yuan Li , “A Study on Electronic Payment Protocols and their Evolution,” *Journal of Information* 2006.11

[7] Xiao Yunpeng,Xu Huimin,Su Fang, “Reserch on Mobile Payment System and Its Security,” *China New Telecommunications* 2005.5

[8] *Modern telecom switching and network*, Shen Jinlong, People post and telecom publishing house 2002 9

Junhong Zhang (1969-), female,Ph D candidate, research direction: e-commerce, information security.
Email: zhangjh@public.wh.hb.cn.

Ping Zhu (1980-), female, Ph D candidate, research direction: parallel and distributed computing, information security.
Email: zhuping@znufe.edu.cn.

Parallel Helmholtz Solver for Chinese GRAPES Atmosphere Model Based on the PETSc Tools*

Guoping Liu, Wentao Zhao, Lilun Zhang
School of Computer Science, National University of Defense Technology
ChangSha, China, 410073
Email: lgpkevin@sohu.com

ABSTRACT

PETSc platform is used as the parallel solver for the complex 3D Helmholtz equations in Chinese GRAPES atmosphere model. With different Krylov subspace methods and preconditioners, we have made numerical experiment for several discrete dimensions. Numerical tests shows that the PETSc tools is an efficient parallel solver library for the difficult 3D Helmholtz equations.

Keywords: Parallel Computing, PETSc, GRAPES, Helmholtz equation

1. PREFACE

1.1 PETSC

PETSc (Portable Extensible Toolkit for Scientific Computation) is developed in American ARGONNE NATIONAL LABORATORY, which has evolved into a powerful set of tools for the numerical solution of partial differential equations and related problems on high performance computing. PETSc is based on MPI parallel library and some mathematics packages, such as BLAS and LAPACK, which is a extending parallel linear, non-linear equation solving tool and time stepping environment. It use object oriented technology which offered gigantic flexibility to users. PETSc is a complex muster of software tools, including many kinds of libraries (like class in C++), PETSc library could be used in application codes compiled by FORTRAN、C、C++, which offer many mechanism needed in parallel application code like parallel matrix and vector gathering program.

The object KSP is the heart of PETSc, it provides uniform and efficient access to all of the package's linear system solvers, including parallel and sequential, direct and iterative. KSP is intended for solving nonsingular systems of the form

$$Ax = b,$$

where A denotes the matrix representation of a linear operator, b is the right-hand-side vector, and x is the solution vector.

1.2 Grapes Helmholtz Equation

GRAPES (Global and Regional Assimilation Prediction Enhanced System) atmosphere model is the new generation of nonhydrostatic compressible forecast model, and it is a self-dependent model developed by the Chinese Agency of Meteorology. The semi-implicit semi-Lagrangian time stepping in this model make it necessary to solve a three dimension Helmholtz equation efficiently, which is very complicated with variable coefficients and cross derivative terms. The continuum and discrete form of this equation is very complex, and make it a intractable problem to solve. In all other nonhydrostatic atmosphere models in the world, the Helmholtz equations is also the computation bottleneck, and till now there is no good final method for it.

With 19 points finite difference scheme, the discrete matrix form of 3-D Helmholtz equations involve three space layers:

$$\begin{aligned}(\xi_{\Pi 0})_{i,j,k} &= B_1(\prod)_{i,j,k} + B_2(\prod)_{i-1,j,k} + B_3(\prod)_{i+1,j,k} \\ &+ B_4(\prod)_{i,j-1,k} + B_5(\prod)_{i,j+1,k} + B_6(\prod)_{i+1,j+1,k} \\ &+ B_7(\prod)_{i+1,j-1,k} + B_8(\prod)_{i-1,j-1,k} + B_9(\prod)_{i-1,j+1,k} \\ &+ B_{10}(\prod)_{i,j,k-1} + B_{11}(\prod)_{i-1,jk-1} + B_{12}(\prod)_{i+1,j,k-1} \\ &+ B_{13}(\prod)_{i,j-1,k-1} + B_{14}(\prod)_{i,j+1,k-1} + B_{15}(\prod)_{i,j,k+1} \\ &+ B_{16}(\prod)_{i-1,j,k+1} + B_{17}(\prod)_{i+1,j,k+1} + B_{18}(\prod)_{i,j-1,k+1} \\ &+ B_{19}(\prod)_{i,j+1,k+1}\end{aligned}$$

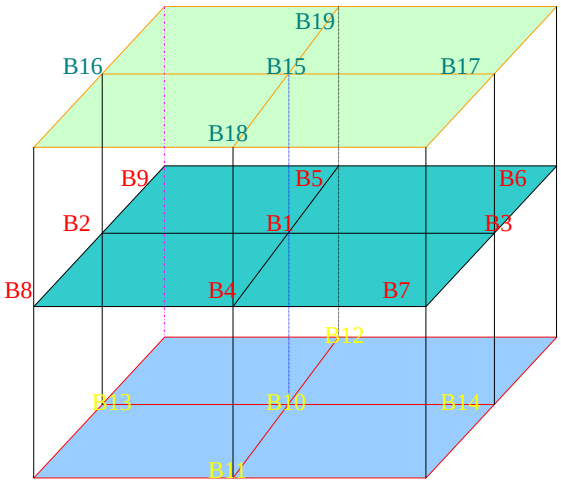


Fig.1. Three space layers of 3-D Helmholtz equations

2. NUMERICAL METHOD

This article only made numerical test for regional ideal field. Global model would be different due to boundary handling. If space grid point of discrete is $m \times n \times l$, we could simpely map the grid points connectings to imitating 19 diagonal matrix A according to i, k, j direction: $(m \times n \times l) * (m \times n \times l)$

This article adopt three groups of data to make test, whose coefficient matrix A and right-hand-side b are produced by GRAPES real data. The data size is: 19285*19285, 39672*39672 and 82080*82080.

Use abundant Krylov subspace mothed and preconditioning in PETSc library to solve $Ax = b$, the key point is the initialization of sparse matrix. The number of non-null of the above three groups data is as:326571、598251、1301935, directly use MatSetValues() function and endow non-null with

* This work was supported by National Nature Science Foundation under grant number 40505023.

value in A.When use PETSc's -log_summary running should choose to statistic solution performance.

Numerical value test is got in a small cluster (have 4 nodes，Each node is double core IA64 CPU and 1.0G memory).
PETSc related parameters are:

a) maximum iterations=10000
b) initial guess is zero
c) tolerances: relative=1e-16
d) absolute=1e-50
e) divergence=10000
f) left preconditioning
g) Using Petsc Release Version 2.3.1

Following the code we show a few of the most important parts of this program.

```
PROGRAM    grapes_petsc
…
/* Initializes PETSc and MPI    */
call PetscInitialize(PETSC_NULL_CHARACTER,ierr)
…
/* Compute the matrix and right-hand-side vector that define
the linear system, Ax=b.    */
call set_A_petsc(a_helm,A,ierr,ids,ide,jds,jde,kds,kde,ims,    &
ime,jms,jme,kms,kme, its,ite,jts,jte,kts,kte) /* Creat matrix. */
call set_b_petsc(b_helm,b,ierr,ids,ide,jds,jde,kds,kde,ims,    &
ime,jms,jme,kms,kme, its,ite,jts,jte,kts,kte) /* Creat vectors. */
…
/* Create linear solver and set various options . */
call KSPCreate(PETSC_COMM_WORLD,ksp,ierr)
call KSPSetOperators(ksp,A,A,                                  &
      DIFFERENT_NONZERO_PATTERN,ierr)
call KSPGetPC(ksp,pc,ierr)
call PCSetType(pc,PCJACOBI,ierr)
call KSPSetTolerances(ksp,tol,                                 &
      PETSC_DEFAULT_DOUBLE_PRECISION,                          &
      PETSC_DEFAULT_DOUBLE_PRECISION,10000,ierr)
call KSPSetFromOptions(ksp,ierr)
/* Solve linear system */
call KSPSolve(ksp,b,x,ierr)
…
/* Free work space. */
call VecDestroy(x,ierr)
call VecDestroy(b,ierr)
call MatDestroy(A,ierr)
call KSPDestroy(ksp,ierr)
call PetscFinalize(ierr)

END

/* About subroutine set_A_petsc and set_b_petsc. */
SUBROUTINE set_A_petsc(a_helm,A,ierr,ids,ide,jds,jde, &
      kds,kde,ims,ime,jms,jme,kms,kme, its,ite,jts,jte,kts,kte)
…
    /* Create matrix A */
call MatCreate(PETSC_COMM_WORLD,A,ierr)
call MatSetSizes(A,PETSC_DECIDE,PETSC_DECIDE,n, &
      n,ierr)
call MatSetFromOptions(A,ierr)
call MatGetOwnershipRange(A,IIstart,IIend,ierr)
call MatSetValues(A,1,nn,1,mm(l),a_helm(l,i,k,j),              &
      INSERT_VALUES,ierr)
…
    /* Assemble matrix A */
call MatAssemblyBegin(A,MAT_FINAL_ASSEMBLY,ierr)
call MatAssemblyEnd(A,MAT_FINAL_ASSEMBLY,ierr)
…
END SUBROUTINE set_A_petsc

SUBROUTINEset_b_petsc(b_helm,b,ierr,ids,ide,jds,jde,    &
kds,kde, ims,ime,jms,jme,kms,kme, its,ite,jts,jte,kts,kte)
…
   /* Create the right-hand-side b. */
call VecCreate(PETSC_COMM_WORLD,b,ierr)
call VecSetSizes(b,PETSC_DECIDE,n,ierr)
call VecSetFromOptions(b,ierr)
call VecSetValues(b,1,nn,b_helm(i,k,j),                        &
      INSERT_VALUES,ierr)
…
   /* Assemble the right-hand-side */
call VecAssemblyBegin(b,ierr)
call VecAssemblyEnd(b,ierr)
…
END SUBROUTINE set_b_petsc
```

3. NUMERICAL RESULT AND ANALYSE

We use T_s to stand for 1CPU's running time, T_{pn} stand for n CPU parallel running time($T_{p1} = T_s$), $S_n = T_s/(n \times T_{pn})$ stand for the coefficient of n CPU parallel running to 1CPU .

Below is the running time stastics under three different data scale, and under different Krylov subspace and preconditioning. In the table: GMRES/JACOBI stand for JACOBI preconditioning when use GMRES subspace method.

Table 1. Running time when A size is 19285*19285

	Tp1	Tp2	Tp4	Tp8
GMRES/JACOBI	4.818E+01	1.742E+01	5.336E+00	4.156E+00
GMRES/SOR	3.879E+01	1.360E+01	3.555E+00	2.579E+00
CR/JACOBI	7.452E+01	4.054E+01	2.501E+01	2.889E+01
CR/SOR	***1.200E+03***	***9.037E+02***	***7.159E+01***	***2.000E+01***
BICG/JACOBI	3.881E+01	1.535E+01	4.932E+00	4.373E+00

Table 2. Running time when A size is 39672*39672

	Tp1	Tp2	Tp4	Tp8
GMRES/JACOBI	2.956E+02	9.616E+01	2.200E+01	1.200E+01
GMRES/SOR	2.789E+02	8.781E+01	1.750E+01	8.558E+00
CR/JACOBI	3.897E+02	1.403E+02	5.010E+01	4.411E+01
CR/SOR	5.579E+02	4.048E+02	3.577E+01	2.138E+01
BICG/JACOBI	2.878E+02	8.319E+01	1.837E+01	9.541E+00

Table 3. Running time when A size is 82080*82080

	Tp1	Tp2	Tp4	Tp8
GMRES/JACOBI	1.399E+03	3.783E+02	1.144E+02	2.638E+01
GMRES/SOR	1.376E+03	3.666E+02	8.989E+01	2.266E+01
CR/JACOBI	1.439E+03	4.042E+02	1.141E+02	3.671E+01
CR/SOR	1.442E+03	4.026E+02	1.086E+02	3.939E+01
BICG/JACOBI	1.388E+03	3.751E+02	9.322E+01	2.490E+01

Through analysing above three table we could get：when use GMRES/SOR we could always get minimum computation time for different data size under different computation size, CR/SOR single CPU running time reach same scalar level as 80280*80280 under data size :19285*19285, computation time

is long when use CR Krylov subspace method, GMRES comparatively shorter.

Table 4. GMRES/JACOBI S_n under different data size

	1CPU	2CPU	4CPU	8CPU
A82080*82080	1.000	1.849	3.057	6.629
A39672*39672	1.000	1.534	3.359	3.079
A19285*19285	1.000	1.383	2.257	1.449

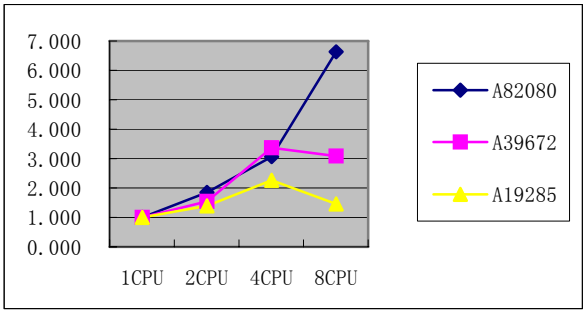


Fig.2. GMRES/JACOBI is the S_n corresponding figure under different data size

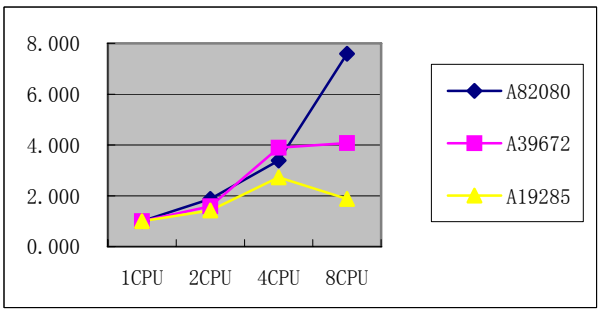


Fig.3. MRES/SOR is the S_n corresponding figure under different data size

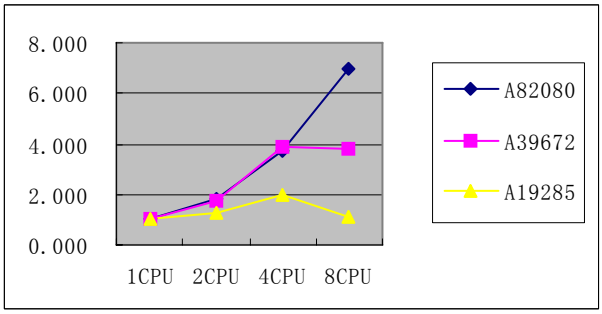


Fig.4. BICG/JACOBI is the S_n corresponding figure under different data size

For most Krylov subspace method and preconditioning , bigger question size, bigger S_n ; Good comparative coefficient could get in handling big questions when many CPU are used at the same time. CR/SOR is not suitable for solving GRAPES mode Helmholtz equation , theoretically CR subspace method require matrix A to be symmetry and positive , obviously GRAPES mode Helmholtz equation is not completely symmetry and positive.

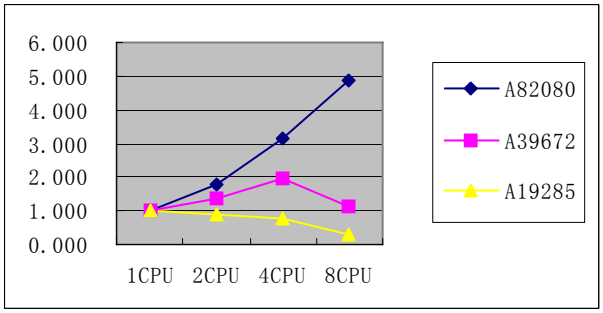


Fig.5. CR/JACOBI is the S_n corresponding figure under different data size

Table.5. CR/SOR S_n under different data size

	1CPU	2CPU	4CPU	8CPU
A82080*82080	1.000	1.791	3.320	4.576
A39672*39672	1.000	***0.689***	3.899	3.262
A19285*19285	1.000	***0.664***	4.191	7.500

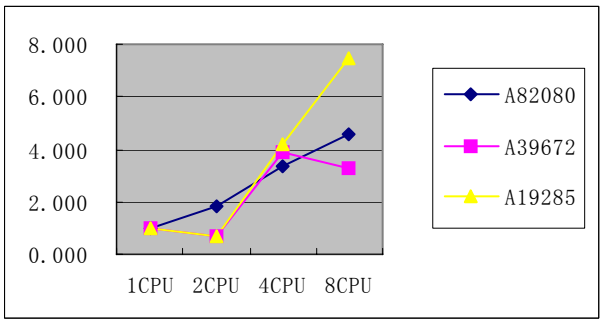


Fig.6. CR/SOR is the S_n corresponding figure under different data size

4. SUMMARY

The PETSc packages make it convenient to use Krylov subspace and preconditioning with no need to consider the details of implementation. We could directly appoint in running which reduced the job of program runner greatly and shortened the development cycle time. At the same time PETSc offer support to FORTRAN、C and C++ which offered gigantic flexibility to users. At present, more and more application programs are developed under PETSc, which shows the high efficiency of PETSc in solving differential equation. GRAPES dynamic mode is a massive data imitating questions which is the advantage of PETSc. We could make good use of PETSc to offer abundant Krylov subspace iterative method and preconditioning to solving core differential equation group in GRAPES for users.

GRAPES dynamic model is using GCR method to solve Helmholtz equation at present. While PETSc library didn't offer support to GCR method directly，but the open source code and expansibility of PETSc make it easy to extend. The high efficiency, flexibility and expansibility of PETSc in solving differential equation would surely play bigger and bigger role in GRAPES.

REFERRENCES

[1]. http://www-unix.mcs.anl.gov/petsc/petsc-as/.
[2]. Xu Shufang,*Theory and Method of Matrix Computation*, Beijing University Press 1995.
[3]. Du Zhihui, *High-Performance Computation Parallel Programming Technology——MPI Parallel Program Design*,Tsinghua University Press 2001.
[4]. Chen Dehui,"A Global and Regional multi-scale dvanced Prediction model,"in N*ational Innovative Research Base for Numerical Weather Forecasting*, 2001.12.

Guoping Liu is master in National University of Defense Technology, the main research direction is parallel computation. The major of bachelor is weather forecast, atmosphere science research.

Strategic Planning of IT Applications in SMEs*

Yanjuan Qiu, Yan Wan
School of Economics and Management, Beijing University of Posts and Telecommunications,
Beijing, 100876, P. R. China

ABSTRACT

The rapid development of information technology and evolving of management concepts, poses big challenges to small and medium-sized enterprises (SMEs), due to their limited human resources, limited capital resources and less developed infrastructure. This paper proposes a hierarchical model for IT strategic planning based on companies' objectives and current status. It then discusses detailed general considerations for SMEs' IT strategy planning, so that SMEs can use them easily to identify their critical needs and decide their IT strategies.

Keywords: SMEs, Strategic Planning, IT Applications, Planning Method

IT application has become an important component of China's information strategy. It is an important means to enhance the competitiveness of enterprises. Facing the fierce market competition, SMEs should be aware of the important role of information technology. Information technology could help SMEs expand their viability, enhance their ability in technological innovation and market competition. With the promotion and support of all sectors of society, more and more SMEs are beginning to understand the value of information technology, and apply IT in enterprises. But more and more fashionable terms emerged recently in IT field, from website, OA to ERP, CRM, SCM, etc, which has given much more difficulties to SMEs in IT applications. Also, the failure of IT applications in some leading companies created a huge negative impact on other enterprises. Under the constraints of finance and human resource, SMEs are generally ignorant with the following issues, such as when do SMEs apply IT? Which field should be the first one to apply IT? How to combine IT with business? How to form a long-term IT strategy to ensure that IT strategy coordinate with business objectives? These issues have become realistic problems stare SMEs in face, yet to be resolved. There is no time to delay to conduct study on IT application in SMEs from the strategic angle.

1. RELATED RESEARCH REVIEW

There are extensive and in-depth research theories about IT application and Information Technology Planning. Such as Stages Theory of IT management by Richard L. Nolan[1], Nolan's model defines the absorption process of IT in enterprises, and gives characteristic of IT at various stages; IBM's Business Systems Planning (BSP)[2] is a summary of information systems development practice; William R. King's Strategy Set Transformation (SST)[3] give us a transformed method from enterprise objectives to IT objectives; Professor John Rockart gave Critical Success Factors(CSF) in late 1970s[4]; Applegate and McFarlan and other scholars gave a method called Strategic Grid(SG) in the early 1980s[5], this method can diagnose and analyze the role of IT with a grid; In his 1985 book Competitive Advantage, Michael Porter introduced a generic value chain model to analyze value chain, namely Value Chain Analysis (VCA)[6]. This method considers business value chain as core, considering internal and external environment to plan information systems, in order to obtain a strategic advantage with information technology. These theories and methods are summary of IT application practical experience, can guide Chinese enterprises using IT to enhance their abilities.

With the expansion of IT application in enterprises, more and more experts and scholars participate in the research of IT application theory and practice. Huacheng XUE[7]-[8] conducts some studies on the IT planning methods and portfolio tactics with his students, and sort various planning methods into four categories according to their character: data center, decision-making center, business process center and project center, and sort these methods into four categories according to the integration process: Bottom-Up, Top-Down, Inside-Out and Middle-Out. Yulin ZHANG [9] give a new analytical framework for strategic planning based on various existing IT planning methods. Lingling ZHANG and Jian LIN [10] base on previous theoretical results, combine with the implementation of China's IT application in enterprises, give a framework of IT/IS strategic planning. These studies also can give some guidance to IT application in enterprises.

However, previous studies and researches are all general practice, paid little attention to SMEs. This paper proposes an IT strategic planning framework for SMEs, and gives a clear appropriate planning method to guide SMEs in their IT applications.

2. AN ANALYTICAL FRAMEWORK OF IT STRATEGY FOR SMES

Firstly, we will analyze the characteristics of IT application in SMEs before the research on strategic planning framework of IT applications for SMEs. Characteristics of IT application in SMEs are determined by characteristics of SMEs. SMEs' characteristics can be understood from two aspects: advantages and disadvantages. There are many theories analyzed the advantages of SMEs, and the large-scale ending theory [11] has the greatest influence. This theory considers that the diversity and individuality of consumption structure leads to the prevalence of small batch production methods. SMEs are more flexible than traditional large-sized enterprises to adapt this mode of production. At the same time, SMEs' have disadvantages of smaller scale, less capital and weaker risk-resisting ability, lack of technology and human resources, lower level of internal management, and unstable organization structure, etc.

All these characteristics require SMEs' IT applications to be right to the critical point, less investment, effective and low-risk. Therefore, in order to meet the overall requirements, IT applications in SMEs must be based on their current situation, building up their systems with mature technologies, instead of catching up with advanced technology and development trend. Secondly, IT application in SMEs should balance the immediate needs with future plans. Thirdly, SMEs should realize the

*The Project is supported by the open fund of Key Laboratory of Information Management and Information Economics, Ministry of Education P.R.C, F0607-10.

balance between the flexibility of their business and the criterion of IT applications. Fourth, SMEs should begin their IT applications in their operational bottleneck and the fields that are needed most.

Based on Strategic Management Theory and previous theories and methods of IT strategic planning, combine with the characteristics of SMEs, we propose a hierarchical framework of IT strategy planning, as shown in Fig.1. Under this framework, SMEs should obtain a clear perceive about the relationship between business strategy and IT strategy, should identify the important factors in IT applications. This framework intends to provide a practical guide to SMEs to set up their IT applications.

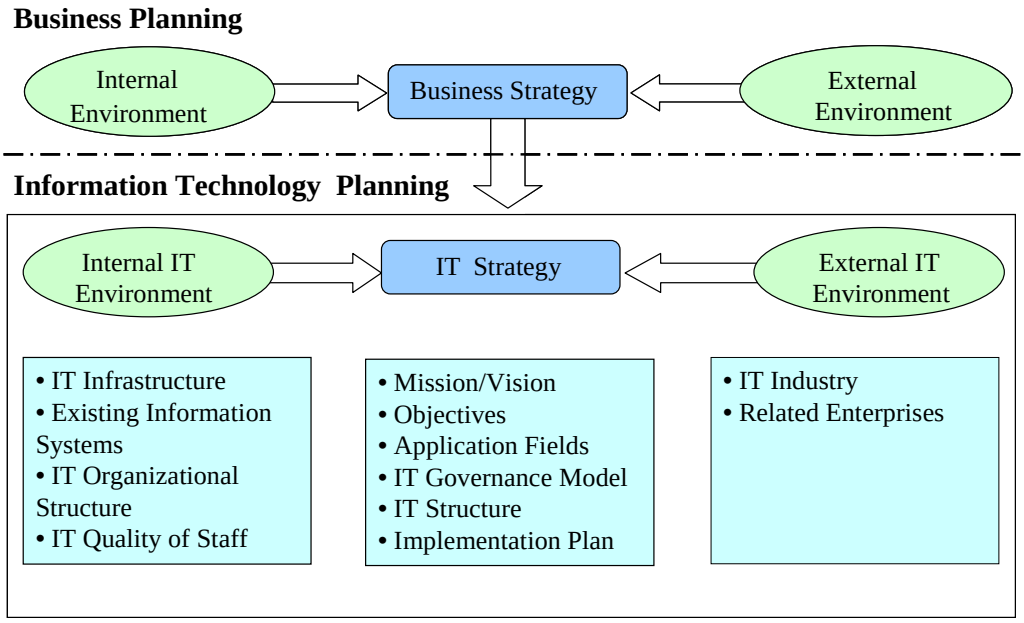


Fig.1. IT Strategic Planning Framework for SMEs

In this framework, we divide IT strategic planning into two levels: business planning and information technology planning. IT strategy should be based on and consistent with business strategy. Therefore, IT strategy planning should be based on business planning to ensure that IT supports the development goals of enterprises. An enterprise should consider its internal and external environment when it plans its business strategy. And also, an enterprise should consider its internal and external IT environment when it plans IT strategy. An appropriate IT strategy can reflect business direction, and successful implementation could make information technology into real play. Thus, there is a two-level implementation of IT strategy in this framework. These two levels constitute a complete IT strategic planning framework, can provide practical guidance to SMEs.

Business planning and implementation of IT strategy form the related environment for IT planning. This model reflects the location of IT planning in the management of enterprise more clearly, and points out the influencing factors and related factors of IT strategy and the content of IT strategy of SMEs.

3. GENERAL CONSIDERATIONS OF IT STRATEGIC PLANNING FOR SMES

Under the IT Strategic Planning Framework for SMEs, we propose a general method of IT planning for SMEs (as shown in Fig.2). It combines with the advantages of the existing IT planning theories and methods, and also considers the special needs of SMEs. Under the resources restriction, information technology and information systems should be chosen carefully for every SMEs.

Conducting IT planning, the SME must have an in-depth understanding of the business strategy. Otherwise IT strategy would deviate from the correct direction easily, and bring losses to the enterprise. Business strategy is the basis of IT strategy, and well understanding of business strategy, SME could get a clear strategic vision and mission.

The internal IT environment of SME include IT infrastructure, existing information systems and quality of staff. It can be considered as its ability of conducting IT strategy. IT infrastructure means the existing computers, networks and other hardware equipment. Appropriate and up to date infrastructure can reduce further investment, and this is especially important for SMEs. Existing information systems are difficult parts because SMEs will have to decide to keep them as a part of the future system or to throw them away. Although keeping them can save cost on the surface, it may cause problems of sharing data with other modules later and limit the capability of future system due to the limitations of this existing system. However, no matter whether the existing hardware or software useful to the new system, good existing systems often indicate that the organization may have good and capable IT staff, and this is a very good and important start point for the new system. The quality of staff is also an indicator of SME's ability of conducting IT strategy. If the staffs have higher quality, the SME can have greater possibility of ensuring the success of IT strategy. SMEs usually have constraints in staff, so this is an important factor to consider before setting up an ambitious plan. IT ability directly affect the choice of IT application objectives. An enterprise with higher IT abilities can choose a more integrated system, while an enterprise with lower IT abilities should start its IT application from the very beginning, and give the employees a certain amount of time to practice to enhance their IT capabilities.

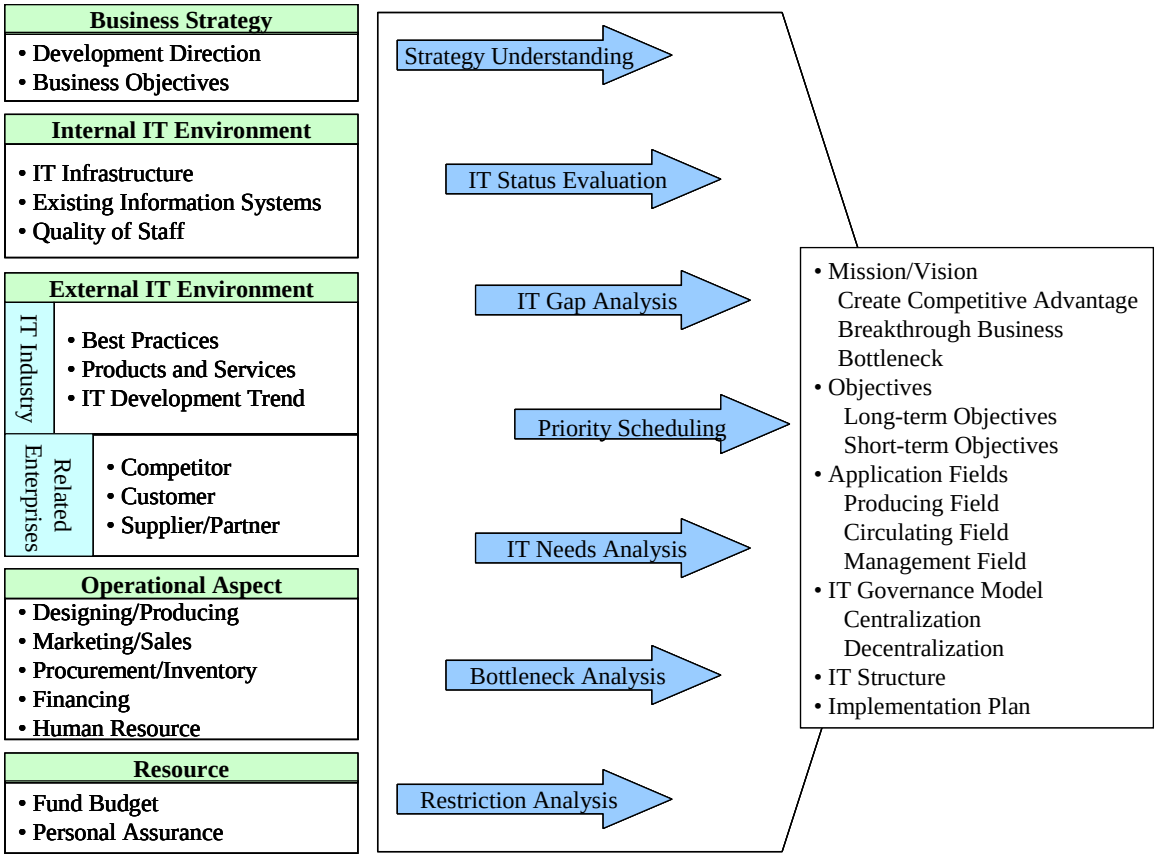


Fig.2 General Considerations in IT Planning for SMEs

The external IT environment of SME include IT industry and related enterprises. Analyzing best practices, products and services and development trend of IT industry, analyzing the IT applications state of competitors, suppliers and customers, the enterprise can find out what is available on the market, what is useful now and what will be useful, and understand external needs, so as to help the company to choose appropriate IT or IS. Since SMEs are vulnerable to risks, they should choose more mature technologies rather than adventuring ones.

The operational aspects of SME include designing/producing, marketing/sales, procurement/inventory, financing and human resource, etc. Analyzing operational aspect bottleneck can find out which area should be the first one to apply IT, and then the second, etc., make its IT application to be "accurately and precisely".
As we all know, the greatest disadvantage of SMEs is lacking of various resources, including funds, human resources, etc. These resource constraints make the most serious influence to IT applications in SMEs. Thus, analyzing the restriction of resources is extremely important to SMEs.

Through strategy understanding, IT status evaluation, IT gap analysis, IT needs analysis, operational bottleneck analysis, restriction analysis and priority scheduling, the enterprise could get a clear IT strategy to guide its IT application. This IT strategy consists of mission/vision of IT application, long-term objectives and short-term objectives, application fields, IT governance model, IT structure and implementation plan, etc. Under the guidance of IT strategy, SMEs can have a clear view of their IT application and make sure the success of these applications.

4. CASE STUDY

As we all know, the practice is the sole criterion of truth. Through the analysis of actual cases, we can test the applicability of this framework and model. In this part, we use the proposed strategic framework and model to analyze the IT strategies of Company A and company B, in order to discuss the applicability of the proposed framework and model.

4.1 Company A

Company A was founded in 2003. This company is a Sino-foreign joint venture, with registered capital of 610,000 U.S. dollars. At present, it has 170 employees, of whom 15 are management. This company mainly produces hydraulic joints and other products. The categories of its products are more than 800 kinds. This company has a monthly production of 300,000-400,000 pieces, and its products are mainly exported to the United States and Britain. It has stable customers, and its sales income was about 17 million in 2004.

According to the proposed framework and model，we give a depth analysis of this company and get its IT strategy as follows:

The mission/vision of IT applications is to breakthrough its business bottleneck. The short-term goal is to achieve a single functional IT application to manage the data of its products, and the long-term goal is to achieve the enterprise's internal information integration, ERP systems can be considered. These information systems need 10-20 thousands, and Company A can afford. This IT strategy can meet its immediate needs, and also takes its future needs into account.

This case proves the feasibility of the proposed framework and model.

4.2 Company B

Company B was founded in December 1994. This company is a state-owned enterprise producing electronic products and integrated electronic energy-saving lamps, with registered capital of 9.15 million. It has a total of more than 700 employees, with a monthly production of 1.5 million lamps and 5 million ballasts. 80%-90% of its products are exported to abroad. Its sales income achieves 250-300 millions since 2002.

According to the proposed framework and model，we give a depth analysis of this company and get its IT strategy as follows:

The mission/vision of IT applications is to create competitive business advantage. The short-term target is to achieve the transformation from IT applications in functional department to the whole enterprise, can choose ERP, CAD, CAM, CAI, etc. This strategy must consider the integration of existing systems and the new systems. The long-term goal is to achieve the integration with external related enterprises, CRM is a best choice. These information systems need 30-50 thousands, and Company B can afford.

Under the guidance of this strategy, Company B conducted its own information technology applications. So far, its information systems run very well, and improve the efficiency of the SME. This proves the applicability of the proposed framework and model.

5. CONCLUSIONS

Base on previous research, we gave a hierarchical framework of IT strategic planning and detailed considerations for IT planning for SMEs. Under the guidance of these framework and method, SMEs can identify critical needs and key application areas according to business goals, operational aspects and management status.

IT applications in China's small and medium-sized enterprises have made certain achievements, but there is still a long way to go. The external environment surrounding them still has problems that hindering the process of IT application in SMEs. Except their own efforts, more helps from the government and other sources would do a lot good to their improvement. A discussion of input from other sources will also benefit this topic.

REFERENCES

[1] Richard L. Nolan, “Information Technology Management Since 1960” in *A Nation Transformed by Information*, ed. Afred D. Chandler Jr. and James W. Cortada (New York: Oxford University Press, 2000): 217-256.

[2] IBM Corporation, *Business Systems Planning Information Systems Planning* [M], New York: IBM Press, 1975.

[3] King, William R., “Strategic Planning for Management Information Systems,” *MIS Quarterly* Vol. 2 No. 1, maart 1978, pp. 27-37.

[4] John Rockart, “Chief Executives Define Their Own Data Needs”, *Harvard Business Review*, March-April 1979: 81-93.

[5] Applegate L. M., McFarlan F. W., McKenney J. L., “Corporate Information Systems Management: Text and Cases,” 4th Edition, Richard D. Irwin: Homewood, IL, 1996.

[6] Porter, Michael E., "Competitive Advantage". 1985, Ch. 1, pp 11-15. The Free Press, New York.

[7] Ziqian PAN, Lihua HUANG, Huacheng XUE, etc., “The Study of The Information Systems Strategic Planning Methods and Its Portfolio Tactics” [J], *Journal of Management Science in China*, 1999, 2(3):43-50(in Chinese).

[8] Qing YAN, Yanqing WANG, Huacheng XUE, etc., “The study of the processes and approaches of integrating business strategy planning and information system strategy planning” [J], *Journal of Management Science in China*, 2000, 3(4): 60-64(in Chinese).

[9] Yuling ZHANG, Jian CHEN, “New framework model for enterprise informationzation strategic planning” [J], *Journal of Management Science in China*, 2005, 8(4): 88-98 (in Chinese).

[10] Lingling ZHANG, Jian LIN, “Model and Frame for Strategic Planning of Information System/Information Technology” [J], *Systems Engineering*, 2001(3):33－36(in Chinese).

[11] Hao BAI, Shanlin YAN, Zengming CHEN, etc., “Study of Informatization Strategy of SME,” [J], *Jounal of Hehai University*, 2006(3):62-65(in Chinese).

Yanjuan Qiu is an Engineer in Telecommunication Planning field. She went in School of Economics and Management, Beijing University of Posts and Telecommunications, and majored in Management Information System in 2000. She graduated from this college and obtained a bachelor's degree in 2004. After that, she continued to study for a master degree in the same university, and graduated in 2007. During graduate stage, she has involved in several research projects, from economic development research to enterprise IT strategy research. Meanwhile, she also presided over the translation of *A Nation Transformed by Information* (New York: Oxford University Press, 2000) with her advisor into Chinese.

Yan Wan is a professor in School of Economics and Management, Beijing University of Posts and Telecommunications, China. She obtained her Ph. D from University of Portsmouth, U.K., in Computer Applications in Management Science. She now engages in teaching and research in Information Management and Information System, Data Mining, Telecommunications Management, etc. and has published many papers in both Chinese and English.

Measuring Information Technology Investments Impact on Technical Efficiency

Lei Yang
School of Business Administration, South China University of Technology
Guangzhou 510640, P. R. China
E-mail: yangl@scut.edu.cn

ABSTRACT

The increasing use of IT has resulted in a need for evaluating the productivity impacts of IT. One of the difficult challenges facing management and researchers today is how to justify costly investments in information technology (IT). This paper presents an approach to investigating the effects of IT on technical efficiency in a firm's production process through a two-stage analytical study. In the first stage, We demonstrate how a mathematical programming technique called Data Envelopment Analysis (DEA) can be used to evaluate the efficiency of IT investments. A nonparametric frontier method of DEA is employed to measure technical efficiency scores for the firms. The second stage then utilizes the Tobit model to regress the efficiency scores upon the corresponding IT investments of the firms. Statistical evidence is presented to confirm that IT exerts a significant favorable impact on technical efficiency and in turn, gives rise to the productivity growth that was claimed by recent studies of IT economic value. Practical implications are then drawn from the empirical evidence.

Keywords: Information Technology (IT), Performance, Technical Efficiency (TE), Data Envelopment Analysis (DEA), Productivity Paradox.

1. INTRODUCTION

Information technology (IT) is re-shaping the competition environment. IT necessitates the establishment of new competition rules that focus more on speed, quality, productivity, efficiency, and customer orientation. Businesses are spending more than ever on IT-related expenditures. For almost two decades, top management has been wondering if IT spending is worthwhile [15]. The issue of measuring IT returns has become even more pressing because the expenditures on IT equipment and service activities have skyrocketed. Remenyi et al. [13] identified several reasons why management needs to scrutinize IT spending. Firstly, the amounts of financial resources invested in IT are substantial and they are thus very likely to supplant other capital spending. Secondly, IT investments are seldom tied to the revenue-generating or profit-making aspects of the business and as a result, management may not readily agree to IT's value, contribution, or performance. Thirdly, IT investments have frequently been perceived as high risk, compared with other traditional capital budgets.

There have been several attempts in the past to assess the impact of information technology on firm performance that have yielded conflicting results. Researchers have been unable to conclude that IT spending by an organization results in increases in key performance indicators. A number of studies on the "productivity paradox" have found a positive relationship between IT investment and firm performance [4, 5]. The research at the industry level has yielded mixed results [2, 6]. This is partly due to the fact that IT is indirectly linked with firm performance. Kauffman and Weill [21A] suggest using a two-stage model to incorporate the intermediate variables that link the IT investment with the firm performance. Wang et al. [16] utilize Date Envelopment Analysis (DEA) to study the marginal benefits of IT with respect to a two-stage process in firm-level banking industry. As a consequence, the issue of how to justify expensive IT investments and substantiate IT's benefits has become important.

There are several ways to define and measure IT's business value. The first type of performance measures that managers understand and may prefer are financial, such as revenues, profits, sales growth, return on assets, return on investment, return on equity, and so on ([3, 7, 11]). Strassmann (1990), however, contends that this bottom-line type of financial metrics may not serve well as valid performance measures to reflect IT's true benefits [15].

A different line of empirical studies considers the intangible IT benefits that were previously overlooked. These focus on user's perceptions, such as acceptance and satisfaction, and try to capture the effect of various user behavioral and psychological constructs, like participation and attitudes, on the successful outcomes of IT/IS projects [9]. These approaches, however, offer no direct links with IT's business value. A framework for assessing the relationship between information technology investments and firm performance is shown in Fig.1.

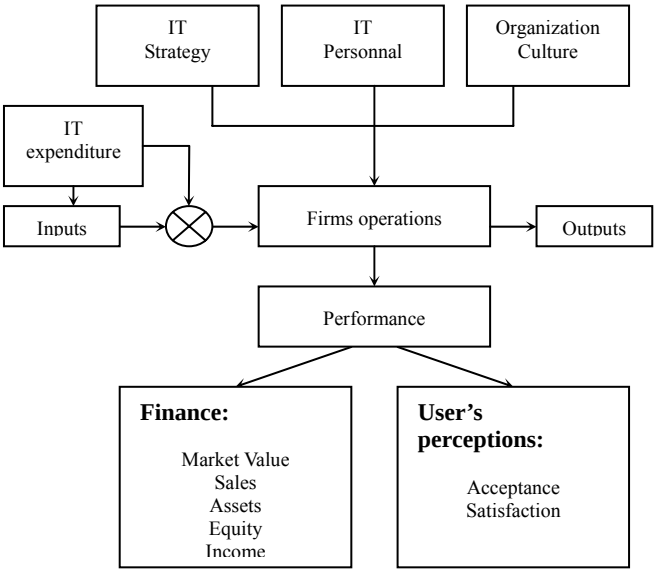


Fig.1. A framework for assessing the relationship between information technology investments and firm performance

Based upon DEA, this paper develops a methodology that measures the relative efficiency of two-stage processes and identifies an empirical efficient frontier. Our work is carried out in two stages. The first stage involves use of data envelopment

analysis (DEA) to construct a nonparametric production frontier and measure the scores of technical efficiency. In the second stage, the efficiency scores are treated as a dependent variable and regressed upon the corresponding IT investments to examine whether IT has a positive influence on technical efficiency.

The current study uses DEA as the fundamental tool for the following reason. First, in performance evaluation, the use of single measures ignores any interactions, substitutions or tradeoffs among various firm performance measures. DEA has been proven effective in performance evaluation when multiple performance measures are present [17]. Second, DEA does not require a priori information about the relationship among multiple performance measures. DEA estimates the efficient frontier from the observations. Third, a number of studies about the IT impact on firm performance have successfully used DEA [14, 16].

2. METHODOLOGIES

2.1 Theory of Production

Firms operate in an exceedingly complex environment, with myriad factors influencing their operations. Their performance is also multidimensional, measurable by many different gauges. Although all this complexity cannot be modeled completely, we believe the framework presented here is reasonably comprehensive, and allows us to pose the following research questions:

(1) Is the gestalt approach valid-that is, can we better capture the relationship between an aggregate of investment measures (both TT and non-IT) and a set of firm performance measures (in lieu of individual variables)?
(2) How are IT investments related to a firm's market value? Market share? Sales? Assets? Equity? Income? What about non-IT investments (labor and capital)? Do these effects vary by industry sector?
(3) What is the impact of computer capital versus noncomputer capital on firm performance?

A firm utilizes different kinds of resources (inputs) and produces tangible goods or intangible services (outputs) to satisfy the needs of its customers. The inputs are also termed production factors and usually include capital, labor, materials, etc. The transformation of inputs into outputs is a production process. The production frontier, which characterizes the relationship between inputs and outputs, specifies the maximum output achievable by employing a combination of inputs. The distance between the maximum output (or the production frontier) and the actual output is regarded as its technical inefficiency.

Technical efficiency is concerned with getting more out of input resources with an extant production technology. In this regard, technical efficiency focuses on either the output side or the input side of a production process. An indicator of technical efficiency can thus be actual output versus expected output (given some input amounts) or resources actually consumed versus resources expected to be consumed (for producing a certain level of output). Productivity indicates the effective use of overall resources, without implying any production technology. Productivity evaluates what come out of the production process against what are consumed to produce them. Productivity growth is then measured as a set of successive indices that compared outputs to inputs. A crucial connection between technical efficiency and productivity can be established: productivity growth is a composite index of the change in technical efficiency and the shift in the production frontiers [10].

Productivity growth=technical efficiency change × technical change

There are two different approaches to measuring technical efficiency: parametric and nonparametric production frontiers. The parametric approach requires the assumption of a functional form (e.g. Cobb–Douglas) to be made for the production frontier; it uses the statistical estimation to estimate the coefficients of the production function as well as the technical efficiency. Nonparametric production frontiers are based on mathematical programming and do not make any assumptions about the functional form. The data points in the data set are compared with one another for efficiency. The most efficient observations are utilized to construct the piece-wise linear convex nonparametric frontier. As a result, nonparametric production frontiers are employed to measure relative technical efficiency among the observations.

2.2 Research Methodologies and Hypothesis

DEA was initiated by Charnes, Cooper, and Rhodes (CCR), and their original model assumed constant returns to scale in the production process. Banker, Charnes, and Cooper (BCC) [1] later proposed an alternative model that can handle the more flexible case of variable returns to scale. There are several inputs X_i (capital and labor, plus an optional IT spending) and one output Y. For any specific firm k, the BCC model is employed to measure the scores of technical efficiency as follows:

$$\begin{aligned} &\min q_k \\ &s.t. \quad -Y_k + \sum_{j=1}^{n} p_{kj} Y_j \geq 0 \\ &q_k X_{ik} - \sum_{j=i}^{n} p_{kj} X_{ij} \geq 0, \quad i = 1, 2, \cdots, s \\ &\sum_{j=i}^{n} p_{kj} = 1 \\ &p_{kj} \geq 0, \quad j = 1, 2, \cdots, n \end{aligned} \qquad (1)$$

where n is the number of firms, and s is the number of inputs.

The purpose of this paper is to introduce to the IT literature a new framework for evaluating investments in IT based on a mathematical programming technique called Data Envelopment Analysis (DEA). DEA is an approach that evaluates the relative efficiency of peer units with respect to multiple performance measures. In DEA, the units under evaluation are called decision making units (DMUs) and the performance measures are grouped into inputs and outputs. DEA is particularly useful when the relationships among the input and output measures are unknown.

To illustrate, the six DUMs plotted in Fig.2 require various amounts of two inputs to produce a specified level of a common output. In Fig. 2, DMUs A, B and C make up the efficient frontier and are considered efficient. DMU E is not considered efficient because while it requires the same amount of Input 2 as DMU B to produce the specified output, it requires more of Input 1. Likewise, DMU F require more of Input 2 and DMU G requires more of both inputs to produce the specified output.

Technical inefficiency in a production process are attributed to a number of events that would unfavorably affect the firm's capacity to transform input resources into output. Some of the

undesirable events are beyond the firm's control, like weather, natural disasters, accidents, regulation changes, etc. Others, however, can be ascribable to the firm itself and be amended through efforts to rectify the situation.

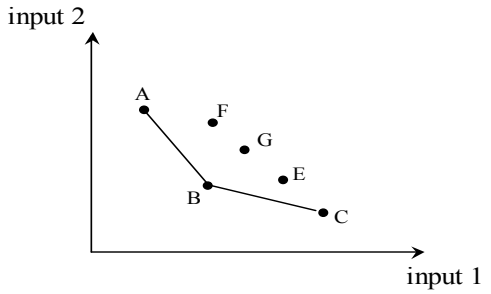


Fig.2. Developing the efficient frontier with DEA

As a consequence, there are reasons for us to presume that the deployment of IT in an organization is able to enhance its capability to produce more output using the same amount of input or, alternatively, produce the same level of output using less input. Therefore, the following hypothesis is implied.

Hypothesis 1. A firm's IT spending has a favorable impact on the technical efficiency of its production process.

Brynjolfsson and Hitt's work was based on standard production theory from economics. The output a firm produces is a function of the inputs it uses. In order to examine IT's impact on technical efficiency in the production process, we carry on the second stage of our study by regressing the scores of technical efficiency, derived from DEA in the first stage, against their respective IT investments. The most efficient in comparison with the others are employed to construct the nonparametric production frontier. Hence, they have perfect scores of one for their efficiency measurement.

McCarty and Yaisawarng [12] suggest that, under this circumstance, the Tobit regression model should be used, because it can account for the censoring of the dependent variable. If, for firm i, we represent the original scores of technical efficiency as TE_i^*, the measured (censored) scores of technical efficiency by DEA as TE_i, and IT spending as I_i, then the Tobit regression model in the second stage is formulated as:

$$TE_i^* = \alpha_0 + \alpha_I I_i + \varepsilon_i$$

$$TE_i = \begin{cases} 1 & if \quad TE_i^* \geq 1, \quad i = 1,2,\cdots,n \\ TE_i^* & if \quad TE_i^* < 1, \quad i = 1,2,\cdots,n \end{cases} \qquad (2)$$

When the coefficient estimate α_I for IT investments is found to be significantly positive, we are provided with statistical evidence to corroborate that IT exerts a positive total effect on the firm's technical efficiency in the production process.

3. DATA DESCRIPTION

A comprehensive firm-level data set is employed in our study. This data set was used in several previous studies to examine the effects of IT on productivity, profitability, consumer value, and substitution elasticities [17].

Analyzing the efficiency of investment in IT is complicated by the fact that (1) there are often a time lag between investment in IT and performance improvement, (2) the length of this lag is not known and in actuality varies, and (3) the performance improvements provided by investments in IT frequently extent beyond one reporting period. To address these issues input data were collected for the years 1989~1991 while the performance measures assessed the compound annual change in the measure over the 5 year period beginning in 1990 and ending 1994. In terms of the three inputs, each was operationalized as the average level of the measure over the period from 1989 to 1991.

A firm's value-added output (Y) is defined as its gross sales deflated by the industry output price deflators , minus its non-labor expenses deflated by the producer price index for intermediate materials, supplies and components. Two production factors, capital (K) and labor (L), were computed as book values of capital stock and labor expenses. The IT-related data were in two parts: IT hardware value (H) and IS staff expenses (S). IT spending (I) was constructed by aggregating H and S. The apparent way of doing this was to add them and use the total to represent the IT spending variable.

We also considered two cases of production factor categorization. For the first, the inputs included the traditional production factors: capital and labor. Thus, IT hardware value was part of capital, and IS labor expenses were included in labor. IT spending was then thought of as an observable firm-specific factor, which influences the firm's capacity of converting inputs into output in the production process. On the other hand, several recent studies of IT economic value have treated IT spending as an individual production factor.We also excluded IT hardware value and IS labor expenses from capital and labor, and considered IT spending as a separate production factor in measuring technical efficiency through DEA. The Tobit regression model then followed to determine the correlation between IT spending and technical efficiency.

4. RESULTS AND DISCUSSIONS

4.1 IT Spending as A Firm-specific Factor

When IT spending is treated as an observed firm-specific characteristic, we are interested in the sign and significance level of the coefficient estimate of α_I in the Tobit regression model. The results from the first stage of DEA for this categorization of production factors (K and L) are presented in Table.1. The BCC model assumes variable returns to scale, and computes the scores of technical efficiency (TE) and scale efficiency (SE) for each firm in the data set. The averages of both efficiencies are presented. Also the numbers of firms with technical efficiency scores equal to 1 are reported. They are used to construct the nonparametric production frontiers for the measurement of technical efficiency.

Table 1. Results of the BCC model with IT spending as a firm-specific factor

Year	Average TE	Average SE	No. of observations	No. of TE=1	α_I (m=3)
1988	0.785	0.951	137	17	0.137 (0.053)
1989	0.787	0.938	133	17	0.101 (0.032)
1990	0.775	0.946	262	30	0.086 (0.023)
1991	0.759	0.911	287	25	0.077 (0.016)
1992	0.765	0.915	296	25	0.054 (0.015)
All	0.735	0.915	1115	31	0.047 (0.007)

α_I shows the coefficient estimates from the Tobit regression model in the second stage. It is observed that all of the coefficient estimates of α_I are significantly positive with the

p<0.01 (actually most of them with the p<0.001). Therefore, we are able to reject the null hypothesis, or the alternative hypothesis of Hypothesis 1 is not rejected, with a confidence level of 99%. In other words, the conclusion represents strong statistical evidence that IT investments, considered as a firm-specific factor, exert a positive total effect on the firm's technical efficiency in the production process.

4.2 IT Spending As A Production Factor

In the second categorization, IT spending is regarded as a production factor, along with capital and labor, in the production process for efficiency measurement. The coefficient estimate of α_I in the Tobit regression model reveals the correlation between IT spending and technical efficiency. For every value of m (1,…,7) used in aggregating IT spending, different scores of efficiency were derived by the BCC model. Table 2 shows only the results for m=3, mainly because this value has been used in most of prior research. The scores of technical efficiency in Table 2. are higher than those in Table.2. These results correspond to one feature of DEA, which states that the addition of an extra input in a DEA model results in an increase in the scores of technical efficiency.

Table 2. Results of the BCC model with IT spending as a production factor (m=3)

Year	Average TE	Average SE	No. of observations	No. of TE=1	α_I
1988	0.812	0.947	137	26	0.098 (0.047)
1989	0.840	0.962	133	31	0.047 (0.023)
1990	0.798	0.950	262	31	0.072 (0.024)
1991	0.794	0.924	287	40	0.071 (0.018)
1992	0.792	0.945	296	43	0.056 (0.017)
All	0.759	0.938	1115	64	0.045 (0.007)

In Table.2. all the coefficient estimates of α_I are observed significantly positive with the p<0.05 (actually most with the p<0.01), thereby allowing us to reject the null hypothesis with a confidence level of 95%. We are again provided with significant results to support our thesis that IT spending, regarded as a production factor here, exercises a favorable impact on the firm's technical efficiency in the production process.

4.3. Discussions

The estimated total effects of IT spending on technical efficiency are found to decrease when the value assumed for m (the multiplier for S in the formulation of I) increases. The average decrease rate is 16.74% when IT spending is treated as a firm-specific factor and 17.55% when IT spending is considered as a production factor.

As m increases, the IS labor component of IT spending becomes more intensive (or the hardware capital component becomes less intensive). This tendency corresponds with the claim made by production economics researchers that technical efficiency and capital intensity commonly are positively correlated. The rationale for promoting a capital-intensive production process is that labor-intensive alternatives would require more labor and at the same time, more capital per output unit, compared with those production technologies with high capital–labor proportions. When labor costs are continually rising and hardware costs dramatically falling, the firm should make good use of this cost advantage associated with hardware [8]. This suggests that in an efficient production process the hardware cost advantage should be capitalized by replacing some labor with hardware, hence, intensifying the hardware component in IT investments.

IT, is expected to enhance an organization's performance as measured by technical efficiency. Previous studies of IT economic value have substantiated the positive correlation between IT investment and a firm's productivity growth and thus, suggested that the IT productivity paradox had disappeared. Due to the connection between productivity and technical efficiency, if management wishes to improve the firm's productivity, one logical way of achieving this is to employ IT in different aspects of the business and enhance its technical efficiency in the production process.

However, management should not draw too hasty a conclusion from our findings. The positive relationship between IT and technical efficiency does not translate directly into reckless IT investments. Firms that invest heavily in IT and are highly efficient in the production process may differ inherently from inefficient firms in ways that are not rectifiable by merely increasing IT expenditure. Strong support from top management, effective IT strategies, innovative organizational culture, excellent IT personnel, and other resources must also be available to help exploit this promised benefit of IT.

5. CONCLUSIONS

Based upon DEA, this paper has focused on the relationship between IT investments and technical efficiency in the firm's production process and employed a two-stage analytical investigation, DEA and the Tobit regression model. Managers can use this new tool to further identify potential candidates for benchmarking and identifying the source of the disparity between IT investment and performance among various firms. We have obtained statistical evidence suggesting that IT, in general, exerts a significantly positive influence on the firm's technical efficiency. Due to the close relationship between technical efficiency and productivity, this study offers another way to explain the productivity paradox associated with IT.

IT is expected to enhance an organization's performance as measured by technical efficiency. Due to the connection between productivity and technical efficiency, if management wishes to improve the firm's productivity, one logical way of achieving this is to employ IT in different aspects of the business and enhance its technical efficiency in the production process.

REFERENCES

[1] R.D. Banker, A. Charnes and W.W. Cooper, "Some models for estimating technical and scale inefficiencies in data envelopment analysis," *Management Science*, Vol.30, No.9, 1984, pp.1078~1092.

[2] A. Barua, C.H. Kriebel and T. Mukhopadhyay, "Information technologies and business value: an analytical and empirical investigation," *Information Systems Research*, Vol.6, No.1, 1995, pp. 3~23.

[3] D.H. Bender, "Financial impact of information processing," *Journal of Management Information Systems*, Vol.3, No.2, 1986, pp. 22~32.

[4] E. Brynjolfsson, "The productivity paradox of information

technology," *Communications of the ACM*, Vol.36, No.12, 1993, pp. 66~77.
[5] E. Brynjolfsson and L. Hitt, "Paradox lost? Firm-level evidence on the returns to information system spending," *Management Science*, Vol.42, No.4, 1996, pp.541~558.
[6] S. Dewan and C. Min, "The substitution of information technology for other factors of production: a firm-level analysis," *Management Science*, Vol.43, No.12, 1997, pp.1660~1675.
[7] B.L. Dos Santos, "Justifying investments in new information technologies," *Journal of Management Information Systems*, Vol.7, No.4, 1991, pp.71~90.
[8] V. Gurbaxani, K. Kraemer and N. Vitalari, "Note: an economic analysis of IS budgets," *Management Science*, Vol.43, No.12, 1997, pp.1745~1755.
[9] W.T. Lin and B.B.M. Shao, "The relationship between user participation and system success: a simultaneous contingency approach," *Information and Management*, Vol.37, No.6, 2000, pp.283~295.
[10] W.T. Lin and B.B.M. Shao, "Relative sizes of information technology investments and productive efficiency: their linkage and empirical evidence," *Journal of the Association for Information Systems*, Vol.1, No.7, 2000, pp.1~35.
[11] M.A. Mahmood and G.J. Mann, "Measuring the organizational impact of information technology investment: an exploratory study," *Journal of Management Information Systems*, Vol.10, No.1, 1993, pp.97~122.
[12] T.A. McCarty, S. Yaisawarng, "Technical efficiency in New Jersey school districts," in: *H.O. Fried, C.A.K. Lovell, S.S. Schmidt (Eds.)*, *The Measurement of Productive Efficiency: Techniques and Applications, Oxford University Press, New York*: 1993, pp.271~287.
[13] D.S.J. Remenyi, A. Money, A. Twite, A Guide to Measuring and Managing IT Benefits, Blackwell, Oxford, UK, 1991.
[14] S.M. Shafer, T.A. Byrd, "A framework for measuring the efficiency of organizational investments in information technology using data envelopment analysis," *OMEGA*, Vol.28, 2000, pp.125~141.
[15] P.A. Strassmann, "The Business Value of Computers," Information Economics Press, New Canaan, CT, 1990.
[16] C.H. Wang, R. Gopaland, S. Zionts, "Use of date envelopment analysis in assessing information technology impact on firm performance," *Annals of Operations Research*, Vol.73, 1997, pp.191~213.
[17] J. Zhu, "Multi-factor performance measure model with an application to fortune 500 companies," *European Journal of Operational Research*, Vol.12, No.3, 2000, pp.105~124.

Lei Yang is an Associate Professor of information management in the School of Business Administration at the South China University of Technology. He received his PH.D. from the Xi'an university in 1997. He has earned a Master of Management Information Systems from the Xi'an University in 1992, and a Bachelor of mechanism engineering from the ChongQing University in 1983. He has published two books, over 50 Journal papers. His research interests are in information management, decision analysis and e-commence.

A Distributed Computing System Applied to Computational Biology

Zuping Zhang, Cengying Fang
School of Information Science & Engineering, Central South University, Changsha, 410083
Email: zpzhang@mail.csu.edu.cn

ABSTRACT

The paper presents a universal distributed parallel computing system--CBDCS, which is based on solving NP-hard problem in Computational Biology and provides an open interface for user to upload application and call service. The system is on-limits and isomerous. CBDCS has the characters such as fault tolerance and usability. The paper mainly focuses on the fault-tolerant mechanism, checkpoint strategy and task scheduling algorithm of CBDCS. The experiment for Motif Finding problem shows that the system can shorten running time sharply. CBDCS is an effective way to solve some NP-hard problems in computing field.

Keywords: Distributed Computing System, Fault Tolerance, Task Scheduling, Java, XML

1. INTRODUCTION

In the research of biology, plenty of problems are NP-hard, the solution often needs large-scale calculation, however the super computer with high-powered is expensive and limited. Along with the development of hardware technology, more and more personal computers have formed a huge network, according to a statistics, up to 2000(It is not so easy to get accurate number from then to now), the number of computers that connect to Internet had exceeded 300 millions, each of them had 80%～90% of its CPU resources left unused, how to organize and use these idle resources for Distributed Computing and solve biological calculation or some hard problems of other fields had became a more and more hot point[1].

We combine the common Characters of Java and Web. We know that Java is irrespective with platform and Web is very easy to use. We adopt volunteer model[2] in our distributed computing system for Computational Biology—CBDCS. It has some characteristics as following:

1) Open: The authorized users can submit the calculation task from network to system and may get results from the calculation resource of this System.
2)Usability: CBDCS offers simple friendly interface, volunteers need to install JRE and client software when they apply for the first time, the other work will be completed voluntarily by client software.
3) Easy programming: Interface is simple and distinct, it is convenient for programming, no need to pay attention to the details, such as fault tolerance and scheduling, etc.
4) Isomerism: CBDCS can run in typical system environment, and may pass through firewall.
5) Fault-tolerance: System can tolerate and handle the faults that made by the uncertainty of volunteers.

2. SYSTEM DESIGN

2.1 System Design Project

*Supported by the National Natural Science Fund of China under Grant No. 60433020.

System adopts the programming language of Java, chooses Java Application and HTTP protocol, spans across various platforms and solves the communication problem through firewall, the communication data encapsulation uses XML technology. Construction of system is showed in Fig. 1.

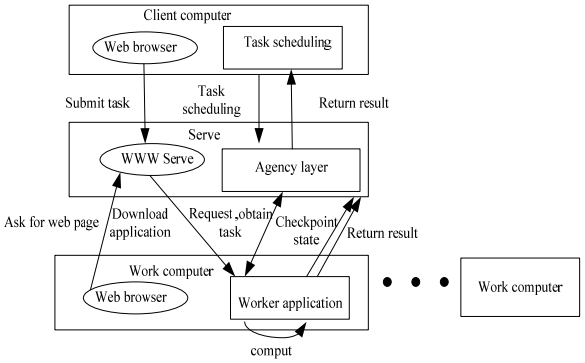


Fig.1. CBDCS Structure

1) Client computer
Client computer is the applicant of resource, it submits problems to server, and waits return result. Users compile the application program that accord with systematic interface, it is uploaded by Web page, server arranges for it voluntarily as one calculation serve, then client computer uploads the scheduling service, server decomposes task and distributes it to each work computer to calculation. When calculation has been completed, it joins the results and return to client computers.

2) Work computer
Work computer offers idle calculation resources, its work process is a circulating process: It applies for task from serve and begins to calculate. It returns calculation result after all task is finished. Work computer downloads client software when it apply for task at the first time, then program applies for task from server voluntarily, calculates and returns result. Terminated application and calculation until volunteer closes computer or has received inform that task be completed. Work computer will preserve intermediate state then send it to server when it need to be pause in the calculating process because system have adopted the checkpoint strategy.

3) Server
Face to client computer, server receives submitted task and returns result. It receives requests from work computers, distributes task, and receives returned intermediate state of checkpoint and calculation results. It offers visited Web interface for client computer and work computer. Besides the work of agency layer--- storing the task set which the apply program decomposes and responding the request of work computer, server adopts suitable scheduling algorithm to distribute task; receiving the result from work computer and validating it. Server receives and preserves the checkpoint state information that is sent by work computer, realizes the transfer of calculation when it is needed.

2.2 System Module And Process

Server and work computer adopt Master-Worker model, systematic module is showed by Fig.2. Application module takes the responsibility for completing the serial part in algorithm, i.e. decomposing problem to be the independent parallel task and returning conformity result. Server Control is the main control module of server and takes charge of interacting with Application module: Offering interface to Application and inserting task produced by Application into database, and scheduling the interface that Application acquiesces to realize and reporting result to Application. TaskServer (Task server module) and FileServer(File server module) actually are the HTTP server which Servlet realizes. The former takes the responsibility for receiving the task which work computer requests and carrying out scheduling of task. The latter takes the responsibility for downloading of program and data file and uploading of result file. The Task table in Database records the detailed information of task, includes task ID, task state, sending time, time restriction, checkpoint information and so on. The there modules of server--ServerControl, TaskServer and FileServer interact by visiting and modifying the Task table. Client is the client serve software that works on work computer.

The whole process of work computer represents in Fig.2.

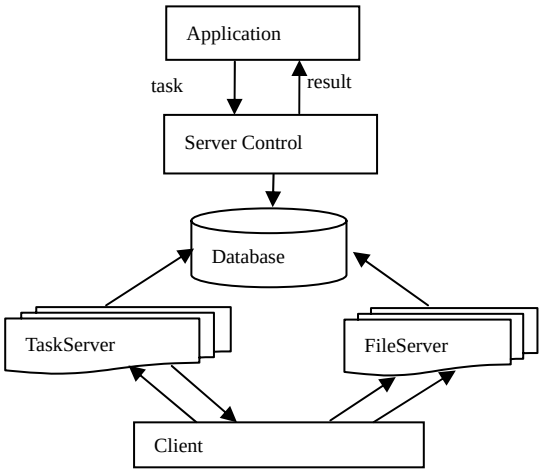


Fig.2. System Module Designed

1) Client sends request message task_request.xml which XML encapsulates to the TaskServer, the request message contains Client's IP of the local work computer, the basic disposition of computer etc.;
2) TaskServer checks the localness of request and judges if the volunteer machine satisfies the minimum requirement of task working, then it carries out the task scheduling, the information of distribute task, includes task ID, program ID that needs to be run, the data file ID which task needs etc., these are encapsulated into the respondence message --task_reply.xml and sends to Client;
3) Basing over the content of task_reply.xml, client sends GET order of HTTP to the designated URL address for downloading corresponding program and data file;
4) Client uploads the result file to FileServer through the POST order of HTTP after calculation.

3. SYSTEMATIC CRUCIAL TECHNOLOGY AND REALIZATION

In the environment of distributed computing, many computers will work in coordination, it will refer to the problems like organization of computers and the distribution of problems, transmission postponement in network environment, fault tolerance etc.. The realization mechanism of some major problem will be given as follow.

3.1 Mechanism of Fault Tolerance

Because of network unreliability and the arbitrariness of volunteer machine joining and leaving, system must consider fault tolerance.

The suitable task of parallel calculation in distributed computing should be coarse-grain, having very high calculation-communication rate, therefore it adopts the mechanism of task redistribution of time out. For the task that had distributed, if it does not return a result in a previously assigned time, system will consider the work computer which the task is distributed to have quitted system or can not complete the task, then it modifies the task state as un-distribution in database, and waits for distribution the next time. The time restriction of each task is designated by Application. ServerControl scans task table periodically, and finds the task of overtime and handles it basing on the sending time of task and the time restriction. This mechanism possible cause that many work computers report a same task result, but the system just accepts the result of returning earliest. Work computer inserts <result_report> into task_request.xml of new task of applying for to report the state of task completion:

```
<result_report>
      <task_id>123</task_id>
      <result_state>0</result_state>
   <!--0 represents success,-1 represents failure-->
   <total_cost_time>45.34</total_cost_time>
   <!- -if successfully processed record total cost time- ->
</result_report>
```

TaskServer analyses <result_report> informs, if task still successful completes at the same time it does not get the result of task.just informs work computer to upload the result ; otherwise it informs not to upload the inform message expresses in <result_ack> of task_reply.xml:

```
<result_ack>
   <task_id>123</task_id>
   <upload_result>0</upload_result>
   <!-0: Should upload result, -1: no need -->
</result_ack>
```

Client in the work computer analyses <result_ack>, uploads when it is need otherwise deletes the result file.

In addition system has considered Byzantine faults, includes: random wrong as having no intention, such as data losing, processor mistake or the failure of network connection and cheat, the attack of malice. It will be solved with following mechanism:

1) The correctness verification of simple task. Some applied results of the parallel task are verified very easily to be correct or false, such as solving certain complex equation, it can be verified so long as returning the result to equation. For those search problems that have only the few solutions, we give the determinant function to judge the correctness.
2) Majority-voting redundancies technology verification. Because of suitable scope limiting of the function level verifying, system will allocate the task for 2**m*-1 times. It requires that at least *m* of them in the result are consistent. Parameter *m* is sets by application program according to accuracy requirement.

3.2 Checkpoint Strategy

Because parallel task is coarse-grain, it needs a long time calculation, once making mistakes, it will waste the plenty of calculations, and we adopt checkpoint strategy to avoid this kind of loss. Duda[3] has proofed that under fault condition if there is not check point the average time of program performing will be increase exponentially with its effective time of performing, and increase linearly when it uses the checkpoint of fix interval. The technology of Checkpoint can not only realize fault recovery but also realize transferring of calculate: using checkpoint to preserve the operation state information on a certain computer, then resuming operates on other computer.

According to the place of the preservation of intermediate state, there are two kinds of checkpoint strategy: local checkpoint model and network checkpoint model[4], the former preserves intermediate result to local, the latter dispatches intermediate result to server, we adopt the latter.

We will first consider opportunity under setting checkpoint. It is periodicity to set checkpoint, and is decided by application program that when it should pause calculation and what state information it should be preserved. Therefore the application program inserts sentence in the suitable recording place of checkpoint, it judges whether there is a time of period from the recent setting of checkpoint. If it is that, we record state information, otherwise calculate continuity. The method that judges if it is time of checkpoint is offered by systematic client.

For realizing the restarting and transferring of calculation, the application program will realize the method of calculation restarting, the information of intermediate state will dispatch to work computer together along with task elephant.

The checkpoint strategy demands to application program realize the interface of checkpoint:

```
public class BasicTask; // Basic kind of task
private object state_info;
// Record the newest intermediate state. For a task that just
    being got, this value is written in by task scheduling
    module. If its value is null, the calculation starts again
    from beginning, otherwise calculation begins from
    breakpoint;
public long start_time
// Calculate the time of beginning;
private CheckCom Thread check_com
// Take the responsibility for the thread communication of
    checkpoint
boolean time_to_checkpoint()
// Judge the time-interval away from to the last checkpoint
    that whether there is a time of period
void do_checkpoint (Object state_tmp)
// After checkpoint is recorded, first we compares the new
    intermediate state information state_tmp with state_info,
    if exists some difference, we start communication thread
    check_com and send it to the  server and replace it on
    state_info()
abstract BasicResult resume()
//Be realized by application programmer, it completes
    reading the state information from state_info of task and
    calculating continuously.
```

3.3 Tasks Scheduling

In CBDCS, we employ the advanced eager-scheduling algorithm for the task scheduling. That is the eager-scheduling algorithm which takes the fault-tolerance (i.e. majority-voting) and checkpoint into account.

Eager-scheduling algorithm: a work computer can only get one task in an application, while the work computer with high operation ability will get more tasks. When the number of tasks are less than the work computers', the tasks that have been distributed but still have not been completed yet will be distributed again, and the fault state of machine will be managed.

Advanced eager-scheduling arithmetic can be described as follow: in the m-voting, every task should be distributed at least for 2*m-1times, then the total 2*m-1results should be validated. Actually, the more effective method is m-first voting method. The method m-first voting[5] starts its check not until the 2*m-1 results come out but when the first m results come back. If the m results are the same, we regard the task has got the right results. For this algorithm, firstly each task will be distributed m times. If these m results are disagree, we distribute them again for m+1 times, until there are m results that are in agreement.

For recording the state of the task and condition of distribution and so on, we design a kind of TaskUnit to encapsulate the task information, ComputeUnit encapsulates the information of each calculation (once a task is allocated for one time, there exist one calculation). Each TaskUnit has a ComputeUnit queue. It allocates one task once, and then adds a ComputeUnit object in the ComputeUnit queue. TaskUnit has defined various states, such as UNSTARTED(task does not still begin to be handled), IN_PROCESS(task waits continued distribution), WAIT_RESULTS(wait some calculations to return as a result), WAIT_VALIDATED(wait the verification of result), HAS_DONE(task has been completed: Get the result after verification or calculation failure).

When we carry out the task scheduling basing to the thought of m-first voting, the frequency of the task number of IN_PROCESS state is less than *m*. Since we hope to get the result of a task as soon as possible, the completed task from task pool can be deleted as early as possible, so we will distribute this kind of task first, then distribute the task that is in UNSTARTED. The scheduling algorithm still handles the task of disabled calculation (time is out and no result has returned), that is to redistribute the overtime tasks that in the state of WAIT_RESULTS. The redistribution is not to redistribute calculation(found the new ComputeUnit object) for task, but is to calculate continuously of the tasks that not be completed---that is to send the newest state information of calculation together with the task to work computer, work computer begins to calculate continuously from breakpoint.

4. CONCLUSIONS

Through test a example sequence when k=10(sequence number), n=82(sequence length), we seek the (15, 4)-Motif (Length of motif is 15, 4 operations are promised) in the sequence, the running result is showed as Table 1.
From the test result, the mechanism of distributed Computing can shorter the run time of programmer sharply.

System not only supports the optimal solution for Computational Biology, but also offers effective way for the NP-hard problem that can be decomposed to in computing field.

Table 1. The running time of multitude work computers

Work computer(Number)	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Running time(Hour)	0.74	0.46	0.25	0.24	0.24	0.17	0.13

REFERENCES

[1] WANG Jian-xin, HUANG Min, LI Shao-hua,"Design and Implementation of a Distributed Computing Platform Based on Task Tree,"in *Mini-Micro Systems*, 2006, 27(5), pp940.

[2] Mei Hao, Shen Zhiyu, Liao Xiangke,"Key Technology of Java Based Distributed Parallel Computing,"in *COMPUTER ENGINEERING & SCIENCE*,2000,22(2), pp103

[3] A.Duda,"The effect of checkpointing on program execution time,"in *Information Processing letters*,1983, 16(4),pp221.

[4] C. Germain, G. Fedak, V. Neri, et al,"Global computing systems,"in *Lecture Notes in Computer Science*, 2001, 2179(6), pp218.

[5] Luis F.G. Sarmenta,"Volunteer Computing [Ph.D.thesis]. Massachusetts,"in *Dept. of Electrical Engineering and Computer Science of MIT*, 2001

Zuping Zhang was born in 1966, he is a professor of Central South University. His research interests main include parameter calculation and application, the fault-tolerance algorithm of network router, large scale database technology.

Cengying Fang was born in 1982, Master graduate student, the current research field of him is bioinformatics.

The Application of Distributed Computing Technique in Rail Transit Automatic Fare Collection System*

Ning Zhang, Liqiang Yang, Tiejun He, Wei Huang
School of Transportation, Southeast University
Nanjing City, Jiangsu Province 210018, China
Email: ningzhang1972@yahoo.com.cn

ABSTRACT

Automatic Fare Collection System (AFC) is one of the most important systems to support the safety and convenience of rail transit operation. But the past research just limited to four layers structure of AFC, which did not fit to Chinese National Standards GB 50381-2006. Based on the four layers structure, a new structure of five layers AFC network was put forward, the performance and reliability of which can be effectively improved by using distributed computing and decentralized data processing technique. The outcome of this study will be helpful to the construction and operation of rail transit AFC.

Keywords: Rail transit,Automatic Fare Collection,Distributed Computing,Decentralized Data Processing

1. INTRODUCTION

During the past few decades, vehicle population has been rapidly increasing in China cities, and the development of traffic supply can not keep up with the increase of traffic demand, so we often encounter traffic jam in cities. To solve this problem, major efforts should be devoted to public transportation [1]. As a kind of safe, convenient, punctual and high efficient transportation, urban rail transit is an effective solution to urban traffic jams. Thus, rail transit systems have been constructed or to be constructed in many Chinese metropolitans. The advantages of rail transit can be supported by Automatic Fare Collection Systems (AFC). The gates in AFC should let the passengers pass as quickly as possible, or else safety and efficiency of rail transit operation can not be guaranteed, just like the congested status which can be seen in the stations in Beijing and Shanghai during rush hours. So is the AFC one of the most important systems to support the rail transit transportation**.**

2. THE DEVELOPMENT OF AUTOMATIC FARE COLLECTION SYSTEM

2.1 The Efinition of AFC

AFC is a revenue collection system [2], which requires the passenger to purchase one ticket and uses it to permit access to or from the rail transit. It is a complicated and huge system, integrated with computers, network, communication, automation, microelectronics, machinery etc, has a wide application in the comprehensive information control system [3]. AFC has some advantages: It automates the ticket counting and selling processes and it can get detailed data on system usage. It also reduces ticket-less travel although it never completely eliminates it, and it allows more revenue to be collected without employing an army of staff. In a word, AFC reduces the need for ticket checking staff and helps prevent fraud.

2.2 The Development of AFC

The oldest version of AFC uses tokens or paper tickets, which are not really “automatic fare collection” systems at all. Then magnetic AFC system was applied in 1970s, the fare media is a magnetic card of credit card size, containing all information necessary for passage encoded on its magnetic stripe. The AFC equipment reads and writes information on the stripe, as necessary. Ticket Vending Machines (TVM) are located in the free areas of stations, which accepts coins, bills, and credit and debit card as payment and issues a ticket for the amount selected; it encodes the ticket for entry. Fare gates are located to separate the free and paid areas of stations. The entry gate establishes the station of origin and other control information for a particular trip; it encodes the ticket for exit. The exit gate subtracts the fare from the ticket value based on the entry station. Point of sale terminal (POST) can be installed in free and paid area according to different functions, which installed in free area of the stations are mainly for selling the tickets, POST which installed in paid area of the stations are mainly for conflicts solving (such as excess fare). Adding fare machines are located in the free areas of stations. The adding fare machine allows value to be added to stored value tickets if the remaining value is less than the required fare at exit. But magnetic AFC system need passengers to insert their magnetic tickets into the slots and then, to take them away at entry and to be recycled at exit, so its operational costs are higher just because the transmitting and recycling mechanical parts were too complicated, which lead to a high maintenance rate (the ratio of annual maintenance costs to the cost of investment) of around 15%[4]. Also magnetic AFC system is poor to expand because it was a centralized system.

In 1990s, Contactless IC card was appeared. compared to magnetic AFC system, it has lower costs, high reliability and high speed to access, and the most important is Contactless Smart card (CSC) AFC system can adopt distributed network, distributed Computing and decentralized data processing technologies. In this system, the passengers would simply touch their IC cards to the reader located in AFC gates and then go through. The less mechanical parts could decrease the maintenance costs [5].

3. DISTRIBUTED AFC SYSTEM

3.1 The Overview of Distributed System

A distributed system is one in which components located at networked computers, communicate and coordinate their actions only by passing messages [6]. This definition leads to the following characteristics of distributed systems: concurrency of components, lack of a global clock and

* This study is started by Program for Tackling Key Problems of Science and Technology (BE2006010) of Jiangsu Science And Technology Department, also supported in part by Program for development of Science and Technology in NanJing (200601001) of NanJing Science And Technology Bureau and Mega-projects of Science And Technology research Plan (8550143007) of Nanjing Metro headquarters.

independent failures of components. In this kind of AFC system, some components fail while others continue to function.

3.2 The Structure of Distributed AFC System

If AFC system adopts distributed network, it can be divided some layers and each layer performs some different functions and exchanges information between layers.

3.2.1 Four Layers Structure of AFC Systems

Distributed AFC system usually consists of tickets layer, terminals (e.g. Gates and TVMs), stations servers and a center server of four layers (Fig.1). The tickets layers include all kinds of Contactless cards, such as single journey tickets, multipurpose smart cards, stored value tickets etc. Terminals mainly are automatic Ticket Vending Machine (TVM), Automatic Gates, Point of Sales Terminal (or POST), Portable Ticket Checking Machine (or PVU) and other terminals etc. Stations servers are Station Computers (SC). The SC consists of a NetServer computer with Raid disc controller, keyboard, mouse and color monitor, CD Reader/Writer drive. Center servers also consist of NetServers and computers which form the Local Area Networks (LAN).

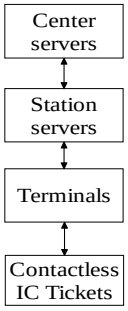


Fig.1. Four layers structure of AFC systems

3.2.2 Five Layers AFC Systems

3.2.2.1 Five Layers Structure of AFC Systems

According to the new National Standards GB 50381-2006, there should be a rail transit AFC Clearing Center (ACC) above the line centers (LC) (Fig.2), just because there may be many operation companies to run their respective lines which should be free transferred in the rail transit network of the city. Some functions of LC are very similar to Center servers in four-layers AFC.

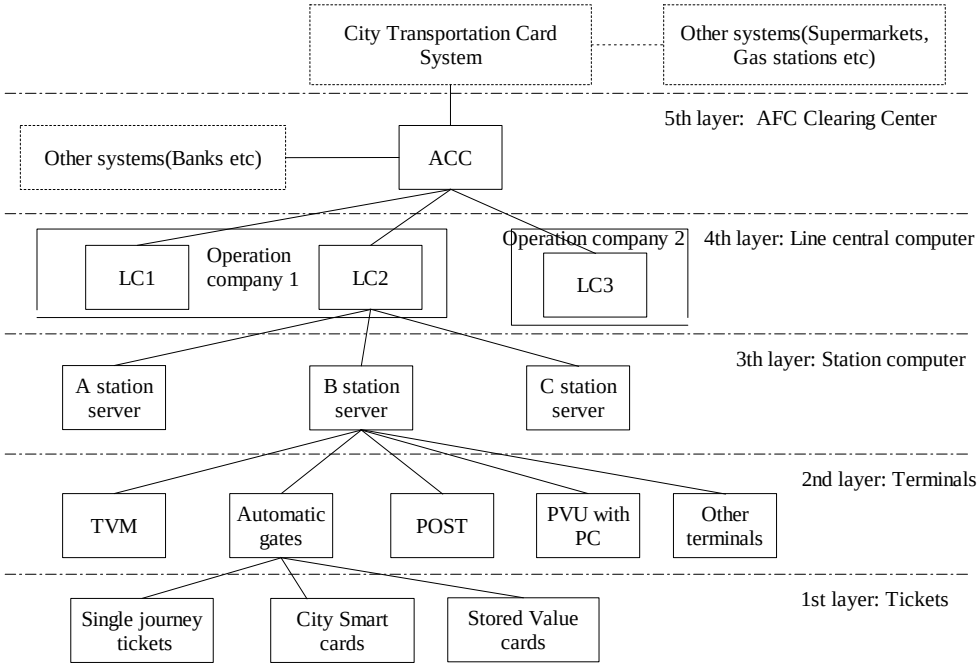


Fig.2. Five layers structure of AFC systems

3.2.2.2 The Functions of Each Layer

In the five layers structure of AFC systems, the functions of the AFC system are distributed to each layer. First layer is tickets layer which is the passenger's payment media, regulating physics and electric characteristics of single journey tickets and stored value tickets, technical requirements of organizing application data structure and security mechanism. Terminals equipped on the concourse of stations serve passengers for entry and exit of the rail transit. The main Fare Ticket Types are Single Journey Tickets (SJT), city smart cards and Stored Value Cards (SVC).

The Station Computer (SC) System, situated at the station level, is responsible for the configuration, monitoring and control of local station equipment, and the data collection within its station. The main functions of the SC are summarized in Table1.

Line Central Computer System (LC) is the central part of Automatic Fare Collection (AFC) on itself rail transit line. It supervises AFC equipments, audits parameterises of AFC equipments, collects data from all equipment types, and generates reports on the activities mentioned above on itself line. It is also responsible for accounting by sending itself data to ACC. The main functions of the LC are summarized in Table 2. All these functions limit to itself line.

The main functions of ACC are to unify the various internal operating parameters of urban rail transit AFC systems. ACC collects CSC and SJT transactions data, AFC audit register data

Table 1. The Main Functions of Station Computer Layer

Functions	Contents
1)Data processing	All kinds of AFC data collection in local station, data processing and upload.
2)AFC Equipment supervision	Equipment control, either manually or automatically; Equipment status supervising and real-time management.
3)AFC Equipment operation management	Equipment Operating Data (EOD) management; Equipment management; Security and key management.
4) Passenger flow monitoring	Monitor real time entry and exit passenger flow in local station; Monitor tickets selling and fare adding.
5) Operation mode management	Setting and dismissing operation modes in local station according to traffic situation.
6) Report creation	Generate activity report by compilation; Various reports (operational, management, traffic and revenue, etc) giving a means to obtain analysis of patron traffic and system performance
7) Revenue management	Managing revenue in local station.
8)Maintain management	Service for maintaining AFC equipments.
9)Software updating	Download new version software and updating.

Table 2. The main functions of the LC

Function
Administration functions
AFC system time synchronization functions
AFC equipment management functions
Spare parts management
Ticketing Key Management Functions
EOD Management Functions
AFC Data Collection Functions
Reporting Functions
Auditing Functions
Information Exchange with ACC
AFC Equipment Monitoring Functions
CSC Ticket Tracking Functions
CSC and SJT Initialization Functions
CSC and SJT Stock Functions
Housekeeping Functions
Network Management Functions

and AFC equipment event logs. ACC is also responsible for revenue settlement among internal rail transit lines and clearing between rail transit AFC systems and city smart card systems. The technical requirements for ticket management, operations management, system operation, system maintenance and management are regulated in ACC.

4. DECENTRALIZED DATA PROCESSING IN AFC

In order to improve the efficiency and reliability of CSC AFC system, decentralized data processing technique was developed[7][8], but those studies only limited to four layers rail transit AFC system. According to the five layers structure of AFC systems discussed above, decentralized data processing is established (Fig.3), where four Data Fields(DF) respectively lies among five layers. A DF is the smallest subdivision of the stored data that can be accessed. A DF can be used to store numerical information such as price, count or date or time for a period of time. A pair of DFs can be used in combination to hold a geo-spatial coordinate. Also, a DF can be used to hold a block of text. A DF takes up permanent storage within the data-store. As DF is applied in AFC, which store data and is a data buffer, when some AFC equipments are failure or busy, data exchange in different layers may be paused, and DF can avoid data losing.

This system is unique with four different DFs featured by various time ranges. In the DF1, wireless communications between CSC tickets and terminals are done within 200

milliseconds while the data flow hourly in the DF2. The data transmission in the DF3 has two cycles: daily and hourly. There are plenty of accounting data among LCs or between rail transit network and city transportation smart card system (also named urban multipurpose transit smart card system), and the data transmission in the DF4 has two cycles: daily and hourly, or even can be adjusted to less than one minute when necessary. These time ranges are varied with system need and aim at both high-speed processing and high reliability [9][10]11]. All the LC computers connect to the ACC through the DF4 and thus, they can exchange data with each other.

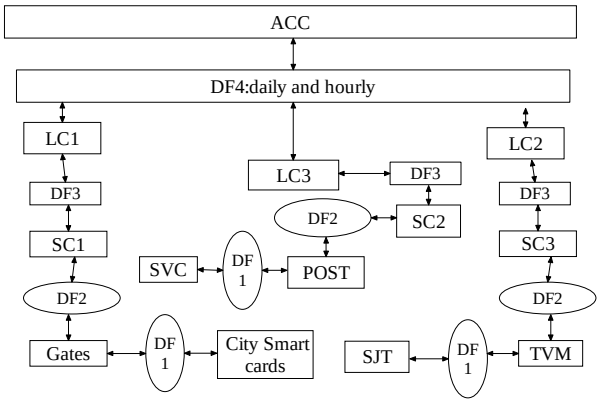


Fig.3. Decentralized CSC AFC system overview

5. CONCLUSIONS

To CSC AFC system, its performance and reliability can be effectively improved by using distributed computing and decentralized data processing technique. Based on Chinese National Standards GB 50381-2006, a new AFC network was designed, it will helpful to let the passengers pass as quickly as possible during rush hours.

REFERENCES

[1] HUANG Cheng,CHEN Chang-hong,WANG Bing-yan etc,"Urban Travel Modal Split and Its Impact on Energy

and Environment,"Journal of Highway and Transportation Research and Development,2005(11), Beijing,pp.163-166.

[2] Http://www.railway-technology.com/glossary/automatic-fare-collection.html.

[3] Feng J uan , Zhao Shimin , Yang Humeng etc. **"**Status Graphics Monitor Technique in Urban Mass Transit AFC," *Urban Mass Transit*. 2006(12),pp. 61-64.

[4] Andre AMPELAS. *Automatic Fare Collection***.** 2001 IEEE Intelligent Transportation Systems Conference Proceedings. Oakland (CA) USA = Aug 25-29, 2001.

[5] Akio Shiibashi, Xiaodong Lu, Kinji Mori. "Achievement of High-speed Processing by Autonomous Decentralized Processing and Decentralized Algorithm in a Wired-and-Wireless Integrated IC Card Ticket System," P*roceedings of the Fourth IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems and Second International Workshop on Collaborative Computing, Integration, and Assurance* (SEUS-WCCIA'06).

[6] George Coulouris, Jean Dollimore, Tim Kindberg. *Distributed systems concepts and design* (3rd edition). Beijing, China Machine Press,2003.

[7] Akio Shiibashi, Fumiaki Mashiba, Kinji Mori. **"**Autonomous Decentralized Processing and Decentralized Algorithm for High Speed in a Wired-and-Wireless Integrated IC Card Ticket System**,"** *Proceedings of the 11th IEEE Symposium on Computers and Communications* (ISCC'06).

[8] Akio Shiibashi, "Fumiaki Mashiba, Kinji Mori. High Reliability in Autonomous Decentralized IC Card Ticket System," *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops* (ICDCSW'06).

[9] K. Mori et al., "Autonomous Decentralized System Software Structure and Its Application", IEEE Fall Joint Computer Conference, pp. 1056-1063, Nov. 1986.

[10] K. Mori, "Autonomous Decentralized System [I-VI]", *IEICE*,Vol.84, No.6-10,2001.

[11] K.Mori,"Technology that flaps in the world Autonomous Decentralized System (1) (2)",The Institute of Electrical Engineers of Japan, Vol. 121,No.2-3,2001, twork security and e-commence.

Research on Design of National Information System for Letters and Calls*

Qifeng Yang , Bin Feng , Zhengwei Cheng , Song Ping
Economics College of Wuhan University of Technology, Wuhan, Hubei, 430070, P.R.China
Email: yangqifengwhut@163.com, 13027154642@vip.163.com, czwdog1120@126.com, songpingwhut@163.com

ABSTRACT

The aim of constructing the national information system for LC is to provide the online complaint service for masses, and to supply relevant governmental institutions with efficient information platform for operation processing and supervising of LC. Besides, it can offer the leaders at all level a public feeling analysis platform. Utilizing the four stages development model of e-government, we proposed the overall plan, vertical and horizontal integration, manage operation mechanism of the system. Moreover, we also suggested the resource information deeply development and application, and its post-evaluation feedback mechanism; and analyzed the draft study method, technological route, emphases, difficulty and innovation; The topological structure and system structure of the system was designed so as to provide theory and method support for the construction of national information system for LC, and other national e-government application system.

Keywords: National Information System for LC, Manage Operation Mechanism,Public Feeling Analysis Platform, Project Post-evaluation

1. INTRODUCTION

The work of Letters and Calls (LC) is an important approach for the Party and government to carry forward democracy, know the public opinion, tie up masses, and to accept the surveillance of the masses. Besides, it is an important way to mediate the contradictions among the people, solve the practical problems, maintain masses' legitimate rights and interests, and to educate and guide the masses. It is useful to maintain the social stability, create nice political environment, construct harmonious society, and promote the decision scientificalness, democratization and legality.
The construction of the national information system for LC will unblock the channel, decrease the unnecessary procedure, and reduce the cost. The user can finish it through the way of letter, visit, telephone or internet.

This system will construct the information system for LC which are inter-institution, trans-regional, electronic, networking, powerful, and resource sharing. Moreover, it will improve the straggling method of institution for LC, and solve the problem in filing and reporting the information of LC to the leaders. This is beneficial for leaders to hold the situation fully, decide scientifically, and deal with the urgent matter on time.
The service function provided for each leader is powerful. The leader can browse the case of LC on the computer everyday, know the dynamic developing trend, supervise the processing of the case, and make comments. However, existing system can't meet the need of the leader. They need not only know the information timely, but also decision support including the intelligent recommendations of relevant information about similar case and early warning of some cases that frequently appear during a specified period, or whose influence are big.

* This item is supported by the National natural science fund item (No. 70572079/G021004).

2. ANALYSIS OF EXISTING CIRCUMSTANCE AND THE STUDY MEANING

2.1 The International And Domestic Analysis of Existing Circumstance

Since 2005, a lot of center leaders, such as, Hu Jintao, Zhou Yongkang, Wang Gang, Hua Jianmin, etc., had made important instructions on many occasions, demanded to accelerate the construction of the national information system for LC, and to structure the national LC information network which would cover the four levels LC organization within two years: the central, the provincial, civic (cantonal), and prefectural. This organization would be interconnection, information sharing, safe and reliable. They also made instructions to construct lot of systems: the swift and unblocked complain accepting system of LC, the unified standard business treatment system, the superintend and checking management system, the LC information analysis and forecast system, the tight system safe security system, the scientific and normal standardized system, convenient and reliable system of the operation system maintenance.

On August 5th, 2006, while listening to state councilor comrade Zhou Yongkang's report about the LC, the General Secretary Hu Jintao had carried on overall arrangement in setting up the information system of national LC, and pointed out that improving and doing a good job on LC should fully utilize information-based tool and means to set up and perfect the information system of the letters. We can construct the central authorities to the level of province first, and then extend to the city (district) and county. The "Decisions of Central Committee of the Communist Party of China about several important problems of structuring socialist harmonious society" expanded the channels of the social situation and people's will expression, perfected the responsibility system of the treatment for the LC, and constructed the national information system for LC. Besides, we should put up diversified forms of communication platform, make masses' interests institutionalized, standardized and legalizing.

January 4th, 2007, "the first stage of the project of national information system for LC" which was undertaken by the Chinese Software and Technological Service Limited Company realized online operation as scheduled. State Bureau for LC and other 17 provinces with the network environment opened and run too.

At present, there are few research achievement on the basis of setting national information system for LC, but some relevant research results based on the department level and area level LC information system can be seen in relevant newspapers and magazines, the survey is as follows: 1) Researches that utilize LC information to serve the leads' science decision. "Making great efforts to explore the effective way by utilizing the LC information to service decisions", in the "Work" of Hunan Province Xiang Tan Standing Committee of Municipal Party Committee, probe deeply into exploring the information resources of the LC, playing a role of the LC, promoting the Party Committee's decision scientific and democratization, studying actively and studying the corresponding way

conscientiously, all these make the LC information become an indispensable important component when the Party Committee makes policy. 2) Researches utilizing LC informationization to serve the people. For example, "The sunshine government affairs", authored by Li Linfeng (2005), "Informationization inserting the wing on the LC", authored by Tiantian (2002), "The Government's LC system goes to the online", authored by Ma Zhongku, Suo Gaoying (2003), both of whom were from the information centre of Shanxi Province. 3) Researches about realizing the technologies of LC information system. "The 'readily accepted' information system in Xuhui District", authored by Shanghai Jiaoda Withup Software Co., LTD. (2006); "The design and realizing of LC office system of Qingdao", authored by Wang Chaojing (2006) who was from the municipal party committee and government computer center of Qingdao; "The design and application of the public security's LC", authored by Wang Limin (2005) who was from the PSB Technology Communications Office in Shenzheng; "The design about the management system of LC in E-government ", authored by Xie Mingjian (2006) etc., there are also some other passages carry on the discussion to this system or the technology realizing or improving of the regional LC information system. 4) The exploring about the impact that the LC information flow does on the regulation of LC: "Information flow in the social stability mechanism---analyzing about management function and democratic function of the regulation of LC' change", authored by Wang Ya'nan(2006); "Sampling analyzing the impact that the information technology does on the government's regulation of LC", authored by Liu Xiaotao(2006).

On abroad, the LC is mostly called public feeling expression. Its aim and function are similar with the LC and its function is distributed in different organization, however the legal status of them is different at all. Karen Layne and Jungwoo Lee (2001), who are from the U.S.A. Nevada Las Vegas University, investigated the E-government building experience in the western developed country, and proposed E-government development models with four stages which were generally approved by the academia and application sector: Cataloguing, Transaction, Vertical Integration and Horizontal Integration, in order to realize the one-stop service and investigate the first stage of the construction. We may know that the project is generally at the Transaction stage. But the complain accepting system of LC inserted in Internet faces Vertical Integration with both business treatment system and superintend and checking management system, two of which were operated in E-government Extranet at present. While the business treatment system, the superintend and checking management system face Horizontal Integration with the application system of E-government that the other government office at the same level have, in order to realize the information interchange and resource-sharing. "Complaints systems worthy of complaint", authored by Nicholas Timmins (2005), has carried on research on the complain mechanism of Britain, has pointed out the present shortcoming of Britain complains mechanism, and explained the thoughts that utilize the information-based means to solve these problems. And Steve Dewar (2005), in "Master of High Court calls for reform of legal complaints system", put emphasis on the importance of information construction in the appealing mechanism reform. Li Yuanjiong (2003) who was from the Seoul city government's Foreign Affairs Office, in "Information technology helping urban government affairs reform---Report on 'applies to deal with the civil administration with online and disclose system' of the Seoul city government ", introduced that as a means to increase the municipal transparency and deeper level of the anti-corruption measures, the government of Seoul developed and ran the "Dealing with Civil administration with online and disclose system "on January 25 , 1999. This system enables each citizen to supervise the dealing situation of LC in 24 hours by the network, can grasp the administrative process without out of the door at any time.

In general, it is a brand-new subject to the study of setting up the national information system for LC. The basic function of the administrative system, such as, the complain accepting system of LC, the business treatment system, the superintend and checking administrative system, has basically realized, but it is facing the Horizontal Integration that the business treatment system, the superintend and checking management system do to the other government offices; and at the basis of those, facing the management and operating mechanism construction of national information system for LC, and also facing the development of the LC information analysis and forecast system, etc.. All of these, involve not only the technology, business and management problems, but also involve deep-seated problems, such as management system, political structure reform, etc. Before this, the domestic and international researches are mostly based on the construction, operation management and information resource-sharing of LC information system on department level, there is not available answer that can be sought.

2.2 The Significance of Studying On Construction of The National Information System For LC

First, there is a great strategic significance to study both the laws about sustainable development of the construction of the LC information system, and master plan. At the present time, the constructions of this system's four stages are almost at the parallel situation, and faces enormous difficulties. Foreign experience shows that the first two phases is relatively easy to achieve, but the vertical integration and horizontal integration are much more difficult, and should be accurate positioning the stage of the LC information system, studying the system sustainable development law, achieving the master plan step-by-step.

Second, it, that study integration and horizontal integration of national information system for LC, is the important part of continuously improving the construction of the LC information system, is also the important technology support to build highly efficient and service-oriented government.

Third, the study on the operating mechanism of the national information system for LC is the key that the national information system for LC runs efficiently, also is the key to construct a efficient service-oriented government. The first stage project of the national information system for LC is promoting overall. In practical terms, the thinking mode, workflow and behavioral habits, which are accumulated by the organization of the LC, the Party Committees at all levels, the government and the legal system related in a long time, in a certain extent, are constrained to play an efficient role in national LC, so it is necessary to rebuild the operation and management mechanism of the national information system for LC, which is a more formidable task than technological innovation, is also the key that the outcome play an important role.

Forth, that, study the depth development and utilizing of the national LC information resource, provide leadership the serves of scientific decision-making, provide individualized advisory services for the masses, is an important manifestation

of constructing a highly efficient service-oriented government and digging the depth effectiveness of the national information system for LC. As the national information system for LC construction is promoting step-by-step, information systems at the national information center will build an information resource data bank which includes the real, complete, standardized and dynamic update national LC information. How deeply to develop and utilize the information resource to provide the scientific decision-making for the leadership and individualized advisory services for the masses has great significance.

Fifth, study the construction of the national information system for LC and the evaluation feedback mechanisms after operation, is of great significance for meeting the needs of leader at all levels, the mass and the staffs working in the LC department, and is also of great significance for efficiently servicing the goal of building a harmonious society.

3. THE MAIN STUDY CONTENT

The study of subject will analyze and combine at the basis of achievements that we already have, according to the four stages development mode of E-government, use the theories and methods, such as information science, management science, public management, E-government, etc., to study the sustainable development law of information system and the master plan; according to the linkage relation that the national information system for LC has with the other E-government application systems, study the horizontally integrate of the national information system for LC; use the theories and methods, such as data warehouse and data excavating , information management , net technology , integration of the information resources ,etc. to study the depth development and utilizing of the national LC information resource, so to provide a warning and predicting public feelings platform for the leaders, and a individualized advisory services platform for the masses; study the project post-evaluation and feedback mechanism of the national information system for LC. The concrete content includes:

(1)Overall plan. According to the four stages model of e-government development, this part takes the international and domestic experience in e-government and e-commerce system construction for reference. Combining with the challenge of LC faced in the period of economic structural readjustment and fast development, it studies on the overall plan and its fractional implement scheme of the national information system for LC. Provide the reference for the system construction.

(2)Vertical and horizontal integration. This part Studies on the vertical and horizontal integration according to the linkage of the system with e-government and other application system. It includes the vertical integration of each level information system, and the horizontal of each level information system with parallel relevant department information system.

(3)Manage operation mechanism based on national information system for LC. It includes the theory basis, the influence of the vertical and horizontal integration on the manage operation mechanism. Besides, it also refers to the activation and constraint mechanism of the vertical/ horizontal cooperation, manage operation mechanism reconstruction of cooperative work for LC, the design of synthetically assessment index system, and the political achievement examine mechanism.

(4)Deeply development and application of national information resource. This part includes the construction of the national information resource base, which refers to application demand and realization tactics, national historical data arrangement and transference tactics, database construction technology and data mining tools. Besides, the public feeling analysis and early warning platform in order to providing scientific decision service for the leaders. This refers to data mining, grid, intelligent recommendation technology, CRM and client experience theory and method.

(5)The post evaluation feedback mechanism of the construction and operation management of the system. It includes the post-evaluation theory, method, assessment index and the feedback mechanism of the system.

4. BASIC IDEA AND METHOD OF THE STUDY ON SYSTEM CONSTRUCTION

(1) Basic idea. The basic ideal carries on according to the route of “overall plan -- vertical and horizontal integration -- manage operation mechanism reconstruction -- information resource base construction and its deeply development and application – project post-evaluation”.

The first step: Combining with the practice, analyze the inherent law of the sustainable development of the national information system for LC. Study on its overall plan.

The second step: The vertical integration can be developed and operated by state bureau for LC unitedly. The horizontal integration relies on the practical application level and concrete condition of each province. It must be developed with regional characteristic. The tactics using uniform interface standard are suggested.

The third step: Take the international and domestic theory and method of development procedure reproduction of e-government. Combine new characteristic of information flow caused by vertical and horizontal integration closely. Fully coordinate existing manage operation mechanism, and reconstruct it on the basis of this.

The forth step: Construct the national information resource base in the information centre of state bureau for LC with the gradually implement of the information system, and then carry on the deeply development and application.

The final step: Study on the post-evaluation of the information system for LC, and build up the feedback mechanism of the project construction and operation management.

(2) Method. Study on overall plan of national information system for LC using the systematic analysis and model methods. Study on the vertical, horizontal integration and the resource sharing using some new technologies such as semantic web, knowledge noumenon, and intelligent grid. Compare and evaluate the manage operation mechanism reconstructed with quondam mechanism using comparative and evaluating methods. Study on the construction of national information resource base using logical model. Study on the public feelings analysis platform, decision support system, information prediction and early warning system using the prediction and statistic methods. Study on the intelligent consulting system, case analysis system, so as to provide the individualized service for the user, using the case reasoning, intelligent recommendation, user

experience theory and methods. Study on the post-evaluation mechanism using level analytic, logic frame, entropy weight optimizing approaches, etc.

5. EMPHASES, DIFFICULTIES AND INNOVATION OF THE STUDY

(1) Emphases. The first is the manage operation mechanism reconstruction based on national information system for LC which decides whether the final aim can be realized or not. The second is the deeply development and application of the national information resource for LC. Especially the public feelings analysis platform, which serves all levels leaders for scientific decision, is an important way to know the problem of LC. The third is the study on project post-evaluation of the system.

(2) Difficulties. The first is that the efficiency of the manage operation mechanism reconstructed for LC need to be tested by the practice and be revised and perfected. This a system project, so we need give an overall consideration and use the measure of "experiment -- evaluation -- perfection -- generalization". The second is that the construction of the public feelings analysis platform relies on the construction of national information resource base for LC witch need to be exact, intact and normative. Because the information construction of the system for LC in different district is uneven, some of them haven't realized digitalization; arduous efforts are needed to carry on the digital innovation.

(3) Innovation. The first is the theory innovation. The "five level goals" of construction of national information system for LC is introduced in this paper, so is the frame system of "overall plan -- vertical and horizontal integration -- manage operation mechanism reconstruction -- information resource base construction and its deeply development and application – project post-evaluation". Besides, the manage operation mechanism for LC which will suit the national system for LC is constructed. The second is idea innovation. Whether the system can be used well, and whether the predict targets of the Party Central Committee, State Department and State bureau for LC rely on the combination of the information technology and the operation for LC, especially on the reconstruction of manage operation mechanism. The third is method innovation. Utilizing the new technologies such as semantic web, knowledge noumenon, intelligent grid, this paper studies the horizontal integration, resource conformity and sharing of the information system for LC. Moreover, it studies on the individualized counseling based on user experience using the intelligent recommendation technology. It also research on the project post-evaluation assessment index of national information system for LC and its data acquiring and processing.

6. SYSTEM STRUCTURE DESIGN

The network topological structure of the national information system for LC is composed of three nets which are internet, e-government extranet and e-government intranet. We can see that it realize the online LC; online cooperative office in the form of "user – provincial (civic, cantonal and prefectural) institution for LC – state bureau for LC" through three net systems which are physical isolated each others.

(1) Portals system Internet online LC: The user submit problem of LC and inquire about the processing result through the portals on internet. The web site nodes, namely the data centre, built on the first stage of the system project are in the provincial institution. While the national system uses the mode of "provincial data concentration".

(2) Cooperative office system provided on the e-government extranet: It can be seemed as a big LAN of e-government. And it is used for the cooperative work of provincial (civic, cantonal and prefectural) and other parallel institutions.

(3) E-government intranet: The data of LC in provincial centre are transmitted to the state bureau for LC as core secret through it. Construct national data concentrating information resource base in order to carry on the system development using relevant technologies such as knowledge management and knowledge engineering. Set up the public feeling analysis platform so as to provide information approach of knowing the public opinion, and decision auxiliary support for the leaders at all level.

The system structure design of the national information system for LC is shown in fig 1. It can be divided into four parts which are external standard layer, application service layer, national information resource base layer and the database layer.

7. CONCLUSIONS

The construction of national information system for LC is a system project and morale project which the Central Party Committee, the State department and leaders at all levels put a high value on. The construction of this system should realize the five level goals of "can be use – know how to use – handy to use – use well – want to use" one by one gradually. Nowadays, the first stage of national information system for LC has got the goal of "can be use" through hard work in system development and test. And it has got the goal of "know how to use" through training of backbone in state bureau for LC and its affiliate institutions in each province. In order to realize the goal of "handy to use", we should carry on the optimization and complete the vertical and horizontal integration.

The goal of first layer to the third layer is limited to the operation and technology ranges, and it's easy to realize. However, how to get the goal of "use well", and how to ensure the information flow, which includes "letters, visits and supervising", operates efficiently and fast through the network need further study. It refers to a lot of departments and institutions, and get involved with the system and mechanism. So the manage operation mechanism should be reconstructed to adapt the national work for LC. Besides, it need the recognition and support of the Central Party Committee, the State department and leaders at all levels, and the combination and innovation of the achievement in information science, system science, philosophy, Party building theory, public management, administrative management, economics, etc. The goal at the fifth level is to realize "want to use". That is to say, the national information system for LC need to satisfy the new, rational, and continuous demand suggested by people, workers of the system and leaders at all levels, and change according to the demand. So, it is a progressive course to set up the construction of the national information system for LC. We should use the tactics of overall planning and implement step by step. This study mainly concentrate on the realization of the goals at third layer to fifth layer, that means how to get the goal of "handy use -- use well – want to use", and stress on the

problem of “use well”.

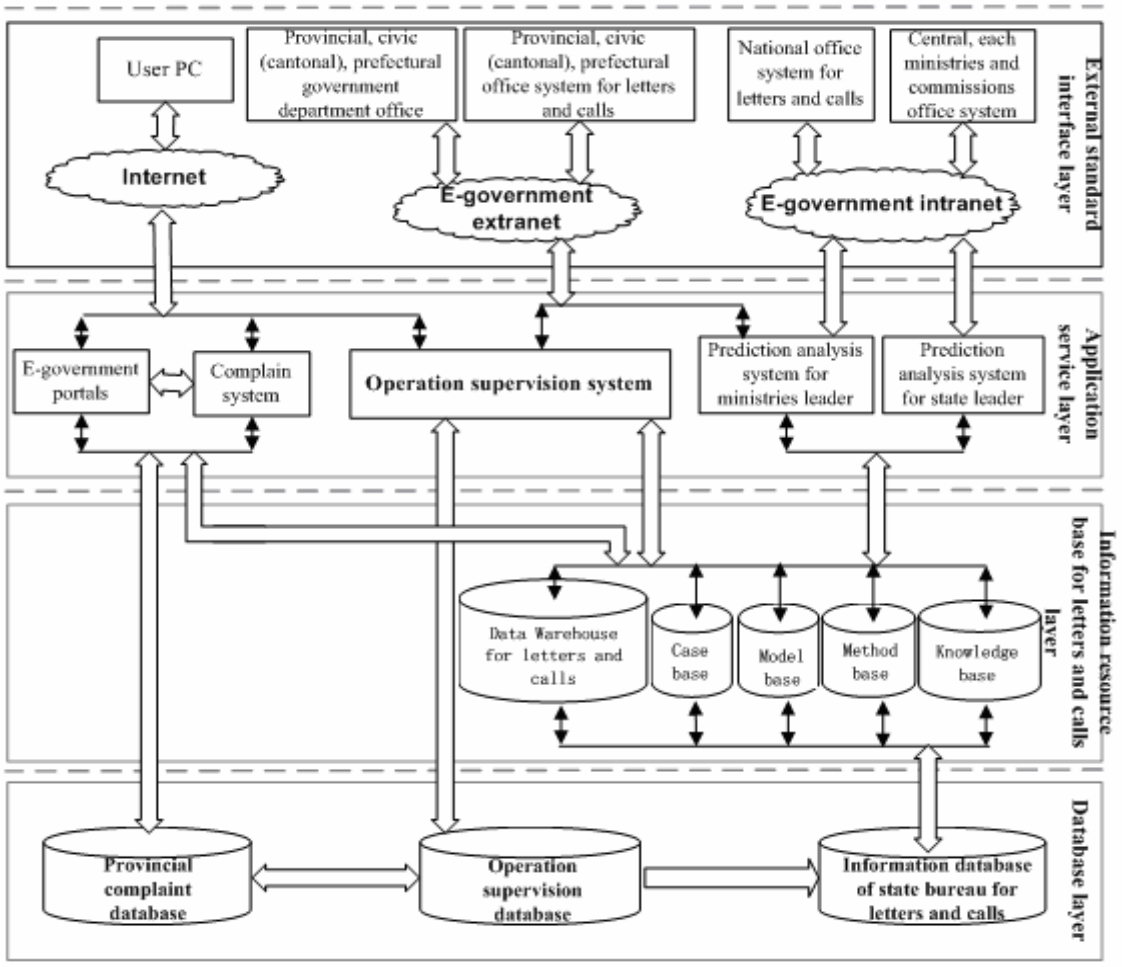


Fig.1. System structure design of the national information system for LC

REFERENCES

[1] Karen Layne, Jungwoo Lee. “Developing Fully Functional E-government：A Four Stage Model,”in *Government Information Quarterly*,2001, pp.122－136

[2] Nicholas Timmins, “Complaints systems worthy of complaint,”in *Financial Times (UK)*,Mar 9,pp.4

[3] Steve Dewar, “Master of High Court calls for reform of legal complaints system,”in *The Irish Times*,Fri,Oct 21

[4] Yun Xiao,“Study on the letters and visits’ information collection and utilizing,”in *Moneychina*,2006.02

[5] Mingjian Xie, “The design about the management system of letters and visits in E-government,”in *Science & Technology Information*, 2006.16

[6] Ya’nan Wang, “Information flow in the social stability mechanism -- analyzing about management function and democratic function of the regulation of letters and visits’ change,”in *Social science forum*,2006.11

[7] Yuanjiong Li, “the Seoul city government's Foreign Affairs Office, Information technology helping urban government affairs reform --Report on ‘applies to deal with the civil administration with online and disclose system’ of the Seoul city government,”in *China e-Commerce Business*,2003.13

Qifeng Yang is an Associate Professor, syndic of Hubei e-commerce institute, expert of e-government and e-commerce in development and reform commission of Hubei and dean of e-commerce in economic college, Wuhan University of Technology. He got the master degree from Hua Zhong University of Science and technology in 1993, and doctor degree from Wuhan University of Technology in 2006. He was a senior engineer in head office of China Construction Bank during 1993-2002, and took part in more than 10 large-scale project of computer application software development, and got 1 first prize, 2 second prize of Science & Technology progress in head office of CCB, and 1 second prize of Science & Technology progress in PBC. Now he takes part in one project of National Natural Science foundation as main member, and takes charge several ministerial projects.

Knowledge Navigation for Digital City Based on Topic Maps*

Jun Zhai, Zhiman Shi, Zhou Zhou, Yan Chen
School of Economics & Management, Dalian Maritime University
Dalian , Liaoning 116026, P.R.China
Email:zhaijun_dlmu@yahoo.com.cn

ABSTRACT

Topic Maps (TM) are standardized by ISO 13250 for the purpose of semantic annotation of WWW resources. This paper presents the knowledge navigation system for city information portal based on Topic Maps technology, including four layers: information resources layer, knowledge layer, information navigation server layer and application layer. The knowledge layer is abstracted from large quantities of distributing heterogeneous municipal information resources by using TM. Navigation scope is built on the knowledge level which enlarges the navigation unit granularity and quantity of receiving information, shortens the navigation routing, and improves the efficiency of navigation. The research is valuable in digital city and knowledge navigation.

Keywords: Knowledge Navigation, Digital City, Topic Maps, City Information Portal

1. INTRODUCTION

The concept of digital world is proposed by the vise president of America and the first international symposium on digital city is held in Beijing [1]. Since the concept of digital city has been put forward, the digital city has aroused the attention of government, increasingly becoming the focus of high-tech development and city construction [2]. In the 863 projects, the ministry of science and technology has set up many subjects to support the research of digital city on theory, technology and industrialization. Construction ministry has built 30 bases of digital city over the country. The digital city has been the focus of academic research in government, enterprises and colleges [3, 4, 5].

City information portal is the important part of digital city construction. City information resources such as data of population, economic, geography and communication usually created and maintained by different departments, so they own the characteristics of distribution and heterogeneousness. Integrating the existed information resources to city information portal, a unified information platform, can bring out more convenient and prompt information service. Generally speaking, city information portal should have following characteristics:

(1) Unified information channel
By unifying the inside and outside relatively dispersive and independent data of city, city information portal can enable the users to access the required information by unified channel, which optimize running of city and improve economic benefits and society benefits.

(2) Powerful content management capability
City information portal can support structure and non-structure data, distinguish data from RDBs, and deal with all kinds of documents.

(3) Individual application service
City information portal can design and provide data and applications, and tailors individualized information portal according to the requirements of users, which enhance the work efficiency of users and reinforce the appetency and attraction for city.

(4) Integrated with existing information system
It is not necessary to redevelopment for city information portal can integrate the existing data and applications, and protect the existing large quantity of investment.

Therefore, information navigation system plays an important role in information content construction and improvement of navigation speed and quality and it is a direct check index for the service quality of city information portal, but most of existing navigation systems only provide cursory content classification and some of them provide information navigation based on keywords, a method of navigation, which is lacking of knowledge and based on information matching, and it exists serious insufficiencies in the rate of complete, precise and expanding.

With the development of semantic Web, information navigation technology based on knowledge appeared, named knowledge navigation, which imports knowledge layer between user interface and information resources to provide the bridge between customers and resources. It not only provides resource view but also knowledge view for users. Knowledge navigation expands the function of the traditional navigation system, and carries out the search service on the semantic level.

Topic Maps are a new ISO standard [6, 7] which used to realize information navigation by efficient organization of information, and now it becomes a mainstream of knowledge management and navigation and been applied in many fields [8, 9].

We apply Topic Maps technology to knowledge navigation of city information portal. The remainder of this paper is organized as follows: first we present Topic Maps basic concepts; then we discuss the method of constructing topic maps by using domain ontology; at last, we describe the framework of navigation system.

2. TOPIC MAPS

Besides the efforts of the W3C summarized by the concept of a "Semantic Web", in 1999 the International Standards Organization (ISO) published a standard for describing WWW resources by some kind of semantic networks. It is called ISO 13250: Topic Maps [6]. Subsequently, it was refined and ported from SGML to XML by the XTM (XML Topic Maps) proposal [7]. Topic Maps are formulated in an XML-syntax, which makes them interchangeable, and, using standard-defined methods and restrictions, mergeable.

Topic Maps allow to describe knowledge and to link it to existing information resources. Topic Maps are described as the "GPS of the information universe", as they are designed to enhance navigation in complex data sets. Although Topic Maps

*This work is supported by the National Natural Science Foundation of China (Grant NO.70540005).

allow to organize and represent very complex structures, the basic concepts of this model –topics, occurrences and associations - are simple.

Firstly, a topic is a construct that represents a real world subject and in this sense a topic can be everything: a theme, a concept, a subject, a person, an entity, etc. A concrete topic is an instance of a topic type. Therefore, a topic and a topic type form a class-instance relationship. At the same time a topic type is also a topic.

Topics have three kinds of characteristics: names, occurrences and roles in associations. The base name of a topic is required. In addition, topics can have a display name and a sort name. These concepts apply to multilingual scenarios or to the use in different geographical.

An occurrence is a link to one or more real information resources, like a web page, a file, a database, a report, a comment, a video or a picture. Generally, an occurrence is not part of a topic map. To express different kinds of occurrences the standard provides the concept of occurrence roles that are topics as well. It is important to notice that topics and nformation resources belong to two different layers. Users may navigate at an abstract level – the topic level rather than directly within data.

Topic associations describe the relationships between topics. They are completely independent of the real information object and represent the essential value-add of the topic map. This concept leads to some conclusions: A concrete topic map can be applied to different information resources. Seen from the other side, different topic maps can be applied to one information resources.

Generally, topic associations are not one-way relationships. They are symmetric as well as transitive and thus, they have no direction. The construct of association types can be used to group topic associations and the involved topics. An association role describes the role of a topic in a topic association. Again, both the association types and the association roles are topics as well.

The Topic Maps standard provides the extended concepts of scope, public subject, and facets.

A scope is a set of topics acting as themes used to control the user-defined validity of topic characteristic assignments. For examples, scopes can be used to qualify topic name characteristics in multilingual topic maps.

A topic may have assigned a public subject descriptor in order to enable the recognition of semantically equivalent topics if topic maps are being merged.

Facets provide a means for annotating information objects pointed at by topic occurrences with simply structured meta-data (property/value pairs). Both properties and property values are expressed by means of topics (facet and facet value type).

Additionally, topic maps can be merged so that their constructs (their topics and associations) belong to one concluding topic map. This can be done via a reference to a topic map B within a topic map A, using the mergeMap-element [7]. Furthermore, two topics A and B are to be merged if both have the same name N in the same scope S or if one topic's subject is identified by the other topic. The standard defines that merging of topic A and B results in a single topic T subsuming all characteristics of A and B (including names, occurrences and association memberships).

3. BUILDING ELEMENTS OF TOPIC MAPS

Topic Maps provide a bridge between the domains of knowledge representation and information management. They build a semantic network above information resources, which allows users to navigate at a higher level of abstraction. One advantage of Topic Maps is that they add semantics to existing data – by organizing and describing them – without modifying them.

We build the elements of topic maps from domain ontology for digital city. The domain ontology, which is the general understanding of domain experts to the knowledge, mainly consists of concepts and relationships. In general, the concepts of domain ontology are the topic types or topics, and the relationships are the associations.

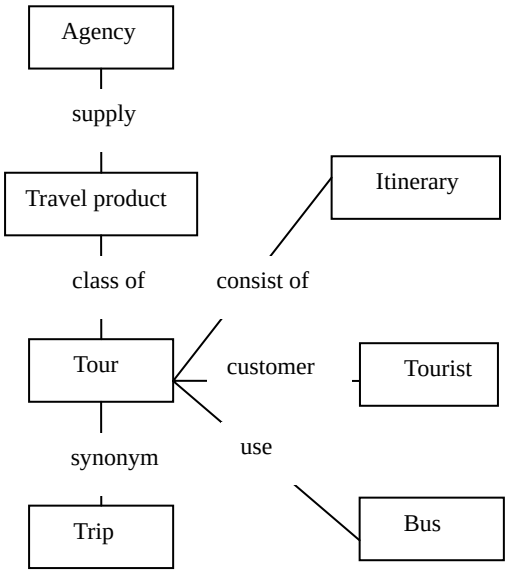


Fig.1. Partial domain ontology for tourist information services

For example, the partial domain ontology for tourist information services is shown in Fig.1. The main concepts include agency, trip, tourist, itinerary etc, and the main relationships include class of, consist of, synonym etc. In XML Topic Map, we code these concepts and relationships as following:

```
<!—definition of Topic Type -->
<topic id="Agency">
<baseName>
<baseNameString>Agency</baseNameString>
</baseName>
</topic>
<topic id="Travel product">
<baseName>
<baseNameString>Travel product</baseNameString>
</baseName>
</topic>
<topic id="Tour">
<baseName>
```

```
<baseNameString>Tour</baseNameString>
</baseName>
</topic>
<topic id="Trip">
<baseName>
<baseNameString>Travel product</baseNameString>
</baseName>
</topic>
……
<!—definition of Association Type and Role Type -->
<topic id="superclass-subclass"/>
<topic id="role-superclass"/>
<topic id="role-subclass"/>

<!—definition of Association -->
<association>
 <instanceOf>
    <topicRef xlink:href="#superclass-subclass"/>
</instanceOf>
 <member>
     <roleSpec>
        <topicRef xlink:href="#role-superclass"/>
     </roleSpec>
        <topicRef xlink:href="#Travel product"/>
  </member>
  <member>
     <roleSpec>
        <topicRef xlink:href="#role-subrclass"/>
     </roleSpec>
        <topicRef xlink:href="Tour"/>
    </member>
</association>
……
```

The following XML statements describe the links between topics and information resources through “occurrence”.

```
<!—definition of Topics -->
<topic id="web site"/>
<topic id="A001">
<instanceOf>
    <topicRef xlink:href="#Agency"/>
 </instanceOf>
<baseName>
    <baseNameString>Dalian    Agency</baseNameString>
 </baseName>
 <occurrence>
    <instanceOf>
       <topicRef xlink:href="#web site"/>
    </instanceOf>
    <resourceRef
          xlink:href="http://www.dalian_agency.com.cn"/>
  </occurrence>
  </topic>
……
```

After building the local topic map from every local domain ontology and information resource, the global topic map for digital city is built through integration process (shown in Fig.2). The integration process follows the rules:

(1) Merging of topics where multiple conceptually equivalent topics are combined into one topic.
(2) Merging associations between topics where conceptually equivalent associations from one topic t1 to another topic t2 are combined into one association.
(3) Copying a topic and/or its properties if the same or equivalent topic does not exist in the target Topic Map.
(4) Generalizing related topics or topic types into a more general topic type.

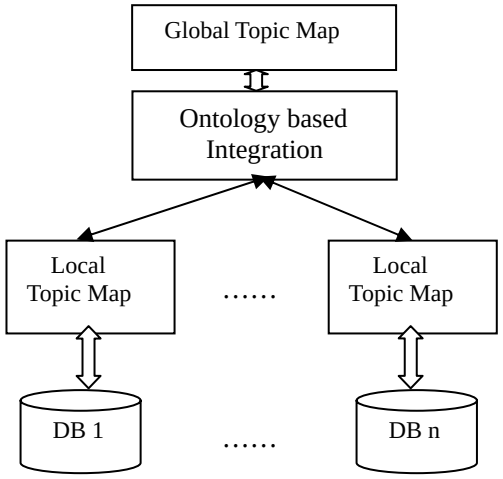


Fig.2. The topic maps integration

4. THE NAVIGATION SYSTEM

In order to map the management of information resources to topic map ontology, knowledge navigation system constructs a knowledge layer above information resources, named topic map ontology, which can be used as the bridge between users and resources. The whole system has four layers (shown in Fig.3): information resource layer, knowledge layer, navigation server layer and application layer.

Information resource layer includes all kinds of resource, such as statistic database, education database, traffic database, tour database and environment database etc.

Knowledge layer is laid over existing information sources for a variety of purposes: location, annotation, connection, comparison, classification, and organization of information. The main characteristics of knowledge layer are:

1) Usually it contains additional information or meta-data about base information elements.
2) It is characterized by a varying degree of structure.
3) It does not modify the base information.
4) As a key characteristic, it contains references to base information elements.

The topic map is well qualified for the knowledge representation. We use relational database to store topic maps which include topic type table, topic table, association table, occurrence table and role table, etc.

Navigation server layer, which is the core of the whole system, completes knowledge management and navigation service. Knowledge management mainly completes the building & maintenance and coding & memory of topic map ontology. Navigation service has two methods: ontology browse and knowledge retrieval. Knowledge retrieval gets back relative resource using semantic matching between the input of user and topic maps. We use TM4J topic maps engine to parse topic maps.

Application layer which is user-oriented graphical interface, realize the functions of login, information issue and knowledge navigation, etc.

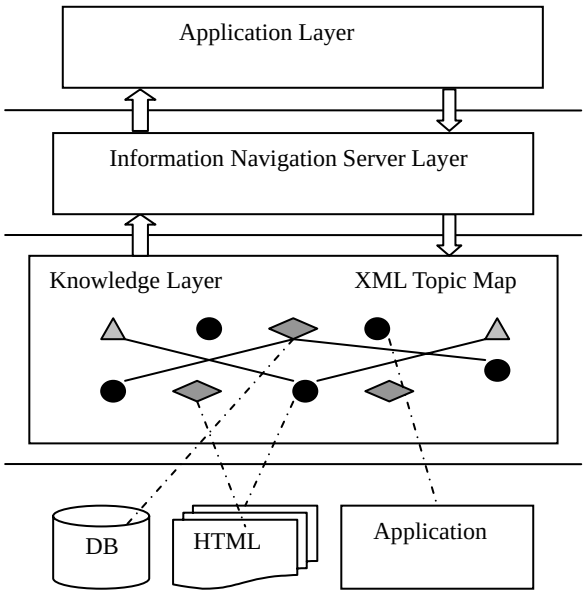


Fig.3. The navigation system framework

5. CONCLUSIONS

Stocks of information and data have grown rapidly in recent years. Yet information seeking has become more difficult and time consuming. Therefore, knowledge navigation is the future development trend for managing city information resource.
In this paper we introduced Topic Maps for city information portal. The topic maps for digital city is built, and then the navigation system framework is presented.
The future research focuses on the automation construction of topic maps from information resources.

REFERENCES

[1] Al Gore. The Digital Earth : Understanding our planet in the 21st Century.
http:/15912261117145/digitalearth/, 1998

[2] Li Qi , Liu Chunbo , Cheng Jicheng. “A Study on Some Theories and Practices of Digital City”. *Geography and Geo-Information Science*,2003,19(1): 32-36. (in Chinese)

[3] Zhang Qiuwen, Wang Cheng, Zhang Yongchuan, Liu Jiping. “Frame and Technology for a Digital City”. *J . Huazhong Univ. of Sci. & Tech.*, 29(7): 13-15. (in Chinese)

[4] Xu Hong,Yang Lixing1,Fang Zhixiang. “Studies on supporting technology systems of digital urban planning”. *Engineering Journal of Wuhan University*, 2002,35(5): 43-46. (in Chinese)

[5] Wang Wenjun, Luo Yingwei,Wang Xiaolin,Liu Xinpeng, Xu Zhuoqun. “A Web Services Based Framework for Spatial Information and Services Integration”. *Chinese Journal of computers*, 2005,28(7): 1213-1222. (in Chinese)

[6] International Organization for Standardization (ISO), 1SO//EC 13250:2000 Information technology - SGML Applications - Topic Maps, Geneva, 2000.

[7] S. Pepper and G. Moore. XML Topic Maps (XTM) 1.0. Topic Maps Authoring Group, http://www.topicmaps.org/xtm, 2001

[8] Petra Wolf, Helmut Krcmar. “Topic Map Technology for Municipal Management Information Systems”. *Proceedings of the 38th Hawaii International Conference on System Sciences*, 2005.

[9] Stefan Smolnik, Ludwig Nastansky. “K-Discovery: Using Topic Maps to Identify Distributed Knowledge Structures in Groupware-based Organizational Memories”. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2002.

Application of Genetic Algorithm to The Position Optimization of The Outriggers for Trimaran

Shunhuai Chen[1], Lianqiong Cui[2]
School of Naval Architecture and Ocean Eng, Wuhan University of Technology
Wuhan, Hubei 430063, China
Email: [1]chenshunhuai@163.com, [2]whutjoan@sohu.com

ABSTRACT

In multi-hulls ship development, the position optimization of the outriggers for Trimaran has to be taken into account. This problem will be solved by multi-objects nonlinear program. In this paper, The Rankine Source method based on the potential flow theory is used to predict the wave-making resistance of the trimaran and the Genetic Algorithms (GAs) is used to optimize the position of the outriggers and the optimum results of CFD method were given too. The results show that GAs is an efficient and qualified engineering optimum design method in ship design.

Keywords: Genetic Algorithm, Wave-Making Resistance, Optimization

1. INTRODUCTION TO *GAS*[1]

The *GAs* developed in the 60~70's of last century by John H.Holland are some kinds of stochastic approach based on the mechanics of natural selection and Darwin's evolutionism, which are known to be robust and global optimum. In basic *GAs,* the problems are transferred to binary numbers called chromosome and fitness number by a kind of coding technique. To engineering problems, it's more convenient to use real numbers instead of binary numbers. The length of the real number string corresponds to the number of design variables. Every string is an individual, which represents a possible solution to the problem. All of the strings consist of a generation. The number of strings is called the population size. The mechanics of survival of the fittest are applied by a kind of fitness value when generate the subsequent generation from their parents. By a series of evolution of the populations, the optimization processes are carried out, and at last the relative optimum solution(s) can be obtained. Suppose P(t) to be the generation t,the standard program structure of GAs shows as follows:

```
Procedure evolution program
Begin
        t←0
        initialize P(t)
        evaluate P(t)
        while (not termination －condition) do
        begin
        t←t+1
        select P(t) from P(t-1)
        alter P(t)
        evaluate P(t)
        end
end
```

2. INTRODUCTION TO RANKINE SOURCE METHOD

To inviscid and irrotational flow, the velocity can be expressed by the gradient of the velocity potential Φ. The ship wave problems can be described as follows:

$$\left.\begin{array}{ll} \nabla^2\Phi = 0 & \\ \Phi_n = 0 & \text{at wetted hull surface} \\ g\Phi_z + \Phi_x\nabla\Phi\nabla\Phi_x + \Phi_y\nabla\Phi\nabla\Phi_y = 0 & \\ & \text{at free water surface} \\ \nabla\Phi = V_\infty & \text{at } \infty \end{array}\right\} \quad (1)$$

The Eulerian coordinate system is used to describe the flow. The global coordinate moves with the ship at the same longitudinal velocity, which origin is chosen at the cross point of centerplane, amidship cross-section and undisturbed waterplane. The x-axis is the cross line of the centerplane and the undisturbed waterplane, which points stern. The y-axis is the cross line of the amidship cross-section and undisturbed waterplane, which points starboard. The z-axis is positive upward. See Fig 1.

It's convenient to rewrite Φ as:

$$\Phi = \phi + \phi_\infty \quad (2)$$

Here, ϕ_∞ is undisturbed potential $\phi_\infty = cx$. ϕ is disturbed potential due to ship hull. Then (1) can be written as:

$$\left.\begin{array}{ll} \nabla^2\phi = 0 & \\ \phi_n = cn_x & \text{at wetted hull surface} \\ g\phi_z + (\phi_x + c)(\nabla\phi\nabla\phi_x + c\varphi_{xx}) & \\ + \varphi_y(\nabla\varphi\nabla\varphi_y + c\varphi_{xy}) = 0 & \text{at free water surface} \\ \nabla\phi = 0 & \text{at } \infty \end{array}\right\} \quad (3)$$

In Rankine source method, ϕ is represented as the potential of source density distribution over the surfaces of wetted hull *(S_h)* and free water *(S_f):*

$$\phi(x,y,z) = -\frac{1}{4\pi}\iint_{S_h+S_f}\frac{\sigma}{r}ds \quad (4)$$

The elevations of free surface, the pressures on the hull surface and the wave making resistance can be obtained by:

$$z = -\frac{1}{2g}(\nabla\phi\nabla\phi + 2c\phi_x) \quad (5)$$

$$p = p_a - \rho(gz + \frac{1}{2}\nabla\phi\nabla\phi + c\phi_x) \quad (6)$$

$$R_w = -\iint(p - p_a)n_x ds \quad (7)$$

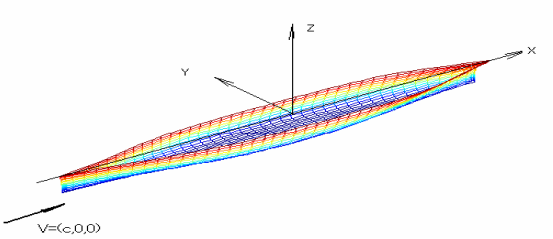


Fig.1. Coordinate system

3. PANELS SYSTEM FOR TRIMANAN

The wigley hull is selected as main hull and outriggers [3].

$$y = \frac{B}{2}[1-(\frac{x}{L_{wl}/2})^2][1-(\frac{z}{d})^2]$$

$$-\frac{L_{wl}}{2} \le x \le \frac{L_{wl}}{2}, -d \le z \le 0 \qquad (8)$$

There are two types of trimarans A and B sketched in Fig 2.

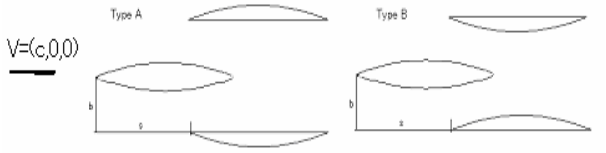


Fig.2. top view of the trimaran

In order to ensure the radiation condition, the source panels for free water surface are moved 2 panel's distance up and 1 panel's distance backward from undisturbed free surface. The panels system is shown in Fig 3.

Obviously (3) are non-linear equations. Different treatment to (3) will obtain different approaches to equations. The linearization equations of (8) are used to speed up the computation, which are reasonable from prediction and optimization point of view.

$$\left.\begin{aligned} \phi_n &= cn_x && \text{at wetted hull surface} \\ g\phi_z + c^2\phi_{xx} &= 0 && \text{at free water surface} \end{aligned}\right\} \qquad (9)$$

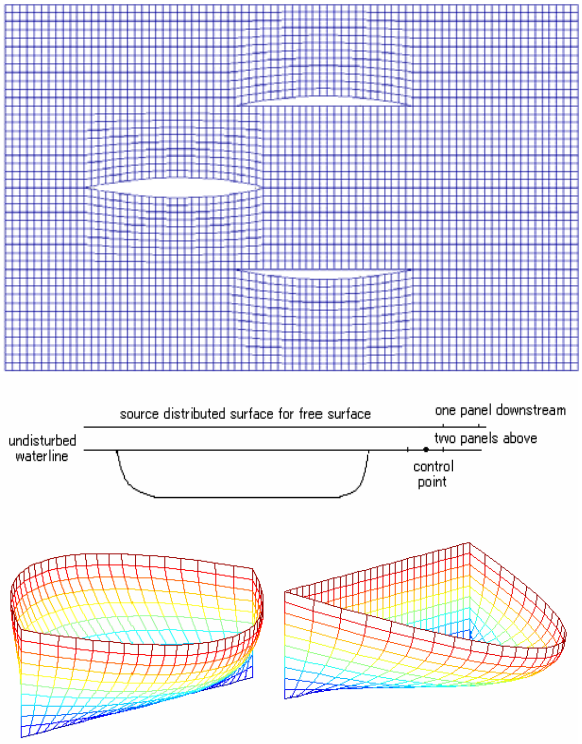


Fig.3. Panels system

Fig4 shows the comparison of resistances between experiments and the calculations. From the Figure we can see that the tendency of the curves is coincident with the experiment data though the absolute values are derived minus from the measured data.

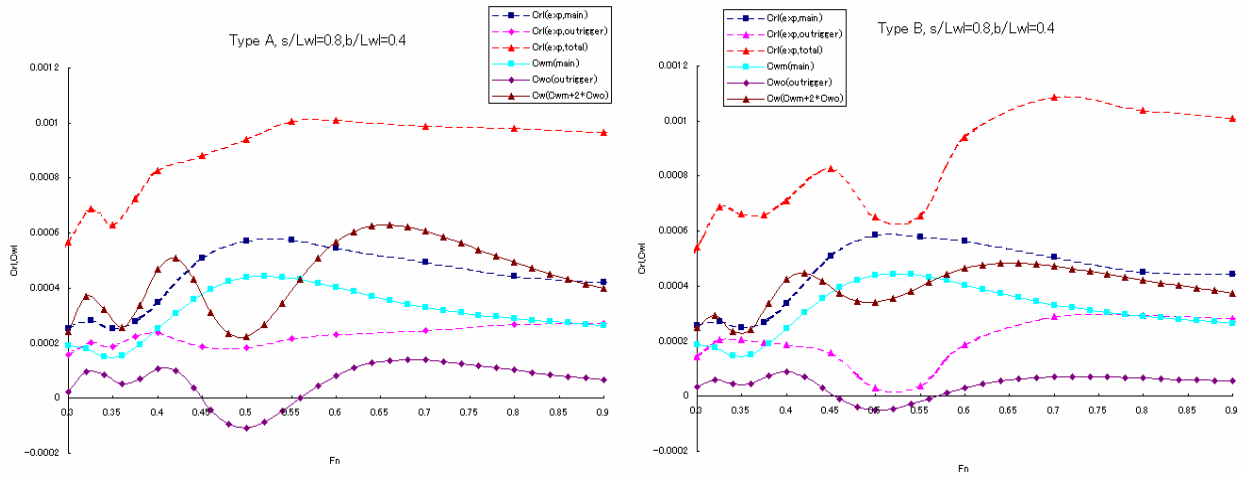


Fig.4. Comparison of wave making resistance coefficient by calculation and experiment

4. THE INFLUENCES OF POSITIONS OF OUTRIGGERS

The locations of outriggers will have great influence on the wave making resistance. To investigate these influences, the calculations are carried out for the trimanan what the outriggers are located in different positions in longitudinal and transverse directions.

1) longitudinal position

Taking Type A as an example, the longitudinal positions of outriggers (s/L_{wl}) vary from 0 to 1.0 while the transverse position being kept in the same value b/L_{wl}=0.4. The results are shown in Fig 5.

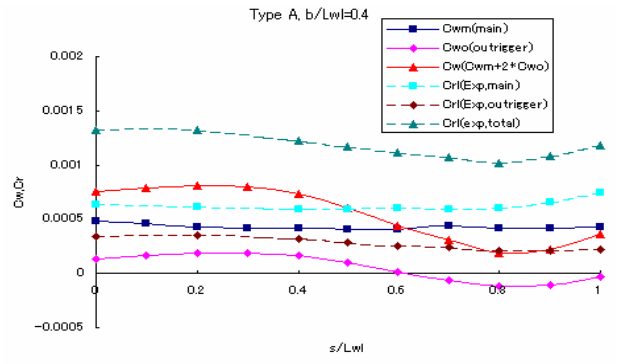


Fig. 5. The influence of longitudinal position of outriggers to resistance

It can be seen that the tendency of the curve is coincident with the experiment data. The optimization value is about s/L_{wl}=0.8. When taking the wave patterns into account, it will be found that at optimization position the outriggers are just located in such positions where the stem of outrigger locates in the area of wave hollows caused by the main hull while the stern locates in the area of humps(refer to Fig 6). It is the same for the Type B.

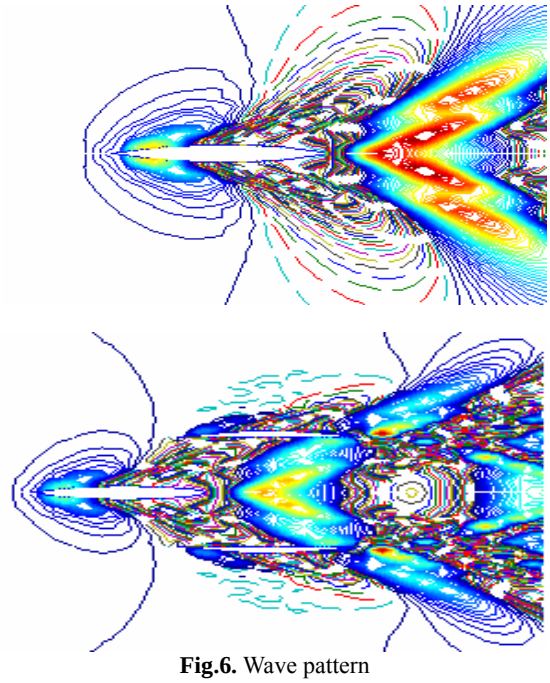


Fig.6. Wave pattern

2) transverse position

The transverse positions of outriggers (b/L_{wl}) vary from 0.1 to 1.0 while the longitudinal position being kept in the same value s/Lw_l=0.8. The results of Type B are shown in Fig 7. The reasonable choice of b/Lw_l is 0.2-0.4. Also when taking the wave patterns into account, it is not difficult to find that in this range the stem of outrigger locates in the area of wave hollows caused by the main hull while the stern locates in the area of humps.

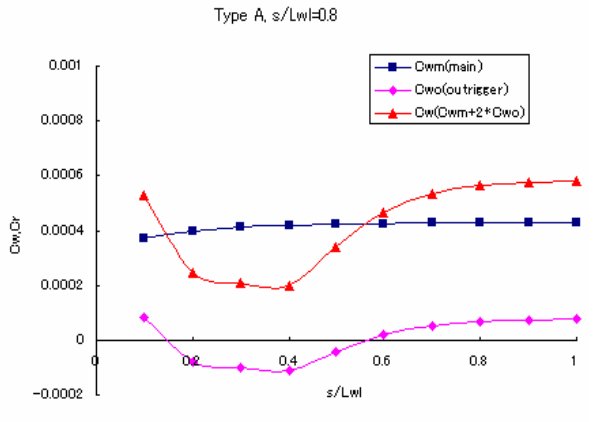


Fig.7. The influence of transverse position of outriggers to resistance

5. GLOBAL OPTIMIZATION FOR POSITIONS OF OUTRIGGER

As described above, the position of outriggers has great influence on wave making resistance. The optimal locations have been discussed above in separate condition. In general, the total resistance (including friction resistance and residual resistance) should be selected as objective from resistance point of view. Considering the fact that the main hulls and outriggers itself have no changes on the present condition, the total wave making resistance can be selected as objective. The relative values b/L_{wl}, s/L_{wl} and the type of trimaran(Type A, B) are selected as design variables to be optimized. Here, the so-called Genetic Algorithms (GAs) are used to get the global resolves.

Fig 8 shows the change of the wave making resistance during the evolution process. The wave making resistance reduces from 2.557E-04 to 9.5736E-05 after 60 generations calculations. In calculation, population size is 5，maximum generation 60，crossover probability0.9，mutation probability 0.1. From Figures we can see that the simulation calculations are efficient. The optimization is that of type B with longitudinal location s/L_{wl}= 0.6874213 and transverse location b/L_{wl}= 0.1836239. Fig9 shows the wave pattern of the last solution, which also shows that the outriggers are just located in the area mentioned above.

6. CONCLUSIONS

(1) It is effective to apply GAs for global optimization of outrigger's position.

(2) The tendency of the curves of wave-making resistance is coincident with the experiment. That shows Rankine source method can be used to predict the resistance of trimaran and do some optimal design at the initial ship developing process

(3) The position of outriggers has great influence on the wave making resistance. Reasonable choice is to located the stem of outriggers in the area of wave hollows caused by the main hull while the stern locates in the area of humps.

(4) For the trimarans shown in Figure 2, the optimal position of outrigger is s/Lwl= 0.6874213 and b/Lwl= 0.1836239. The reasonable type is B.

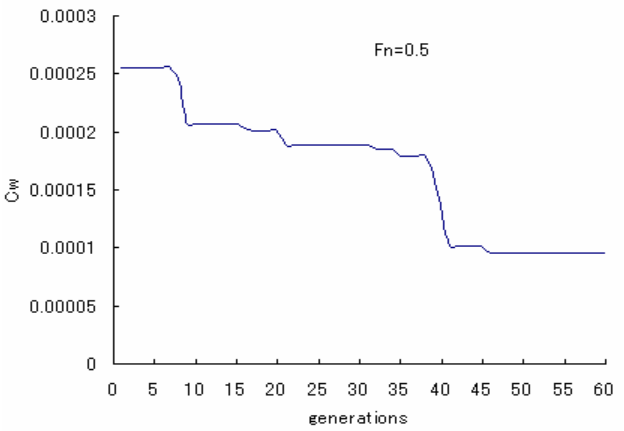


Fig.8. Process of evolution by Gas

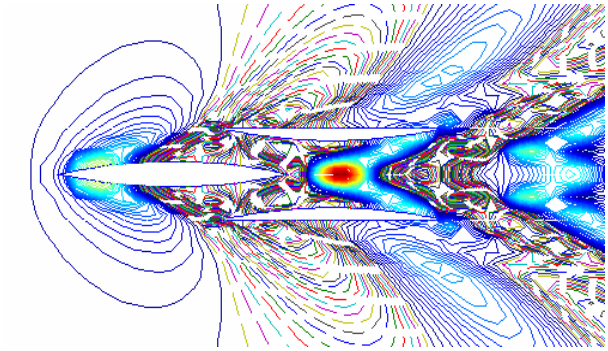


Fig.9. Wave pattern with optimal position

REFERRENCES

[1] Goldberg D E Genetic algorithms in search, "optimization and machine learninn[M]," Canada, *AWPC Inc*,1985.

[2] Dejhalla R,etc. "Application of genetic algorithm for ship hull form optimization," *Shipbuild Progr.*2001.48.

[3] Wilson M B Hsu C C,Jenkins D S. "Experiments and predictions of the resistance characteristics of a wave cancellation miltihull ship concept," *33rd American Towin Tank Conference*,1993,103~112.

Shunhuai Chen is a a Full Professor and a head of Ship Design lab in School of Naval Architecture and Ocean Eng., stangding superintendent of the institute of Naval Architecture and Ocean Engineering, Wuhan University of Technology.

Lianqiong Cui, female, born in 1983. She is a master degree candidate of School of Transpotation, Wuhan University of Technology. Her research interests are in Application of Genetic Algorithms to Ship Design.

QoS Multicast Routing Algorithm Based on Modified Particle Swarm Optimization

Hong Zhang [1], Wenbo Xu [2]
[1]School of Mechanical Engineering
[2]School of information Engineering, Southern Yangtze University
Wuxi 214122，P.R.China
Email: [1]jndxzh@sohu.com; [2]Email:xwb@sytu.edu.cn

ABSTRACT

Because of its NP-completeness of QoS routing problem, many heuristics such as Genetic Algorithms are employ solve the problem. Base on Particle Swarm Optimization (PSO), this paper presents a Modified PSO to solve QoS multicast routing problem. We test MPSO-based routing algorithm on a network model. For performance comparison, we also test the original PSO algorithm. The experiment results show the availability and efficiency of MPSO on the problem and its superiority to PSO.

Keywords: QoS Multicast Routing, NP-Complete, PSO, Mutation

1. INTRODUCTION

Multicast is a communication service that allows simultaneous transmission of the same message from one source to a group of destination nodes. To implement a multicast session, a network must minimize the session's resource consumption while meeting the quality of service (QoS) requirements. QoS multicast routing relies on state parameters specifying resource availability at network nodes or links, and uses them to find paths with enough free resources. An efficient allocation of network resources to satisfy the different QoS requirements is the primary goal of QoS-based multicast routing. However the inter-dependency and confliction among multiple QoS parameters makes the problem difficult. It has been demonstrated that it is NP-Complete to find a feasible multicast tree with two independent additive path constraints.

Generally, heuristics are employed to solve this NP-complete problem. Some Genetic Algorithms (GAs) have been used to solve the problem form different aspects. GA reassures a higher chance of reaching a global optimum by starting with multiple random search points and considering several candidate solutions simultaneously.

Particle Swarm Optimization (PSO) is a recently proposed novel heuristic method [5]. In this paper, we will employ a Modified PSO (MPSO) with mutation operation to solve the Multicast QoS routing problem. The paper is organized as follows. In Section 2, the network model of QoS multicast routing problem is introduced. The origin and the development of PSO are described in Section 3. Section 4 is our proposed MPSO-based QoS multicast routing algorithm. The experiment results are given in Section 5 and the paper is concluded in Section 6.

2. PROBLEM STATEMENT

A network is usually represented as a weighted digraph G = (V, E), where V denotes the set of nodes and E denotes the set of communication links connecting the nodes. |V| and |E| denote the number of nodes and links in the network, respectively, Without loss of generality, only digraphs are considered in which there exists at most one link between a pair of ordered nodes [6].

Let $s \in V$ be source node of a multicast tree, and $M \subseteq \{V - \{s\}\}$ be a set of end nodes of the multicast tree. Let R be the positive weight and R+ be the nonnegative weight. For any link $e \in |E|$, we can define the some QoS metrics: delay function delay (e): $E \to R$, cost function cost (e): $E \to R$, bandwidth function bandwidth (e): $E \to R$; and delay jitter function delay-jitter (e): $E \to R^+$. Similarly, for any node $n \in V$, one can also define some metrics: delay function delay (n): $V \to R$, cost function cost (n): $V \to R$, delay jitter function delay-jitter (n): $V \to R^+$ and packet loss function packet-loss (n): $V \to R^+$. We also use $T(s,M)$ to denote a multicast tree, which has the following relations:

$$delay\ (p(s,T)) = \sum_{e \in p(s,T)} delay\ (e) + \sum_{n \in p(s,T)} delay\ (n) \quad (1)$$

$$\cos t(T(s,M)) = \sum_{e \in p(s,M)} \cos t(e) + \sum_{n \in p(s,M)} \cos t(n) \quad (2)$$

$$bandwidth\ (p(s,T)) = \min(bandwidth\ (e)), \quad e \in p(s,T) \quad (3)$$

$$delay\text{-}jitter(p(s,T)) = \sum_{e \in p(s,T)} delay\text{-}jitter(e) + \sum_{n \in p(s,T)} delay\text{-}jitter(n) \quad (4)$$

$$packet\text{-}loss(p(s,T)) = 1 - \prod_{n \in p(s,T)} (1 - packet\text{-}loss(n)) \quad (5)$$

where $p(s,T)$ denotes the path from source *s* to end node *t* in T(s, M). With QoS requirements, the problem can be represented as finding a multicast tree T(s, M) satisfying the following constraints

1. Delay Constraint: delay(p(s,T))≤D;
2. Bandwidth Constraint: bandwidth(p(s,T))≥B;
3. Delay-jitter Constraint: delay-jitter(p(s,T))≤J;
4. Packet-loss Constraint: packet-loss(p(s,T))≤L;

QoS multicast routing problem is a NP-complete hard problem, which is also a challenging problem for high-performance networks.

3. PARTICLE SWARM OPTIMIZATION

Particle Swarm Optimization (PSO), originally proposed by J. Kennedy and R. Eberhart [5], has become a most fascinating branch of evolutionary computation. The underlying motivation for the development of PSO algorithm was social behavior of animals such as bird flocking, fish schooling, and swarm theory. Like genetic algorithm (GA), PSO is a population-based random search technique but that outperforms GA in many practical applications, particularly in nonlinear optimization problems. In the Standard PSO model, each individual is treated as a volume-less particle in the D-dimensional space, with the position and velocity of *i*th particle represented as Xi=(Xi1,Xi2,...XiD) and Vi=(Vi1,Vi2,….ViD). The particles move according to the following equation:

$$V_{id} = wV_{id} + c_1 rand(\cdot)(P_{id} - X_{id}) + c_2 Rand(\cdot)(P_g - X_{id}) \quad (6)$$

$$X_{id} = X_{id} + V_{id} \quad (7)$$

where c_1 and c_2 are positive constant and rand() and Rand() are two random functions in the range of [0,1]. Parameter *w* is the inertia weight introduced to accelerate the convergence speed of the PSO. Vector $P_i = (P_{i1}, P_{i2}, \cdots, P_{iD})$ is the best previous position (the position giving the best fitness value) of particle *i* called ***pbest***, and vector $P_g = (P_{g1}, P_{g2}, \cdots, P_{gD})$ is the position of the best particle among all the particles in the population and called ***gbest***.

4. THE PROPOSED PSO

4.1 Coding

The coding is one of important problems to solve the QoS multicast routing problem using Modified Particle Swarm Optimization (MPSO) algorithm or PSO algorithm. It involves encoding a path serial into a feasible solution (or a position) in the search space of the particle. In this paper, we design an integral coding scheme for MPSO so that it can be employed to solving the discrete combinatory optimization problem. In our scheme, the number of paths (no loop) reaching each end node t∈M are worked out. With the number of end nodes denoted by $|M|$, the number of paths to end node *i* is represented as $n_i (1 \le i \le |M|)$. The paths to end node *i* can be numbered by an integer variable $t_i (1 \le i \le |M|)$,where $t_i \in [1, n_i] (1 \le i \le |M|)$. Therefore we can obtain a $|M|$-dimensional integral vector $(t_1, t_2, \cdots, t_{|M|})$ denoting a possible path serial with each component t_i varying in the interval $[1, n_i]$. In the MPSO for QoS Multicasting routing problem, such an integral vector represents the position of the particle and the combinatory optimization problem is reduced to a $|M|$-dimensional integral programming.

The initial population is a matrix with row vectors representing particles' positions. The dimension of a row vector is the number of end nodes. The value of the *i*th component of a row vector denotes the number of a path from the source node to end node *i*, which is initialized by randomly select an integer number in the interval, $[1, n_i]$.

4.2 Fitness Function

In our proposed method, the fitness unction is defined as:

$$f(x) = \frac{\omega_1}{\text{cost}(T(s,M))}(\omega_2 * f(d) + \omega_3 * f(j) + \omega_4 * f(p)) \quad (8)$$

where ω_1 , ω_2, ω_3 and ω_4 is the weight of cost, delay, delay-jitter and packet loss, respectively; f(d), f(j) and f(p) are defined as

$$f(d) = \prod_{t \in M} F_d(delay\ (p(s,t)) - D) \quad (9)$$

$$F_d(delay(p(s,t)) - D) = \begin{cases} 1, delay(p(s,t)) < D \\ \alpha, delay(p(s,t)) \ge D \end{cases} \quad (10)$$

$$f(j) = \prod_{t \in M} F_j(delay\_jitter\ (p(s,t)) - J), \quad (11)$$

$$F_j(delay\_jitter(p(s,t)) - J) = \begin{cases} 1, delay\_jitter(p(s,t)) < J \\ \beta, delay\_jitter(p(s,t)) \ge J \end{cases} \quad (12)$$

$$f(p) = \prod_{t \in M} F_p(packet\_loss\ (p(s,t)) - L) \quad (13)$$

$$F_p(packet\_loss(p(s,t)) - L) = \begin{cases} 1, packet\_loss(p(s,t)) < L \\ \sigma, packet\_loss(p(s,t)) \ge L \end{cases} \quad (14)$$

where $F_d(x)$, $F_j(x)$ and $F_p(x)$ are penalty functions for delay, delay-jitter and packet loss, respectively, and α , β and σ are positive numbers smaller than 1.

4.3 MPSO for QoS Routing Problem

As demonstrated by F. Van den Bergh, original PSO is not a global convergent algorithm, which makes PSO apt to encounter premature convergence [1]. In this section, we propose a Modified PSO (MPSO) with mutation operation exerted on global best particle. The operation employed in this paper is Gaussian mutation described as follows.

$$P_{gd} = P_{gd} + \sigma \cdot N(0,1) \qquad (d = 1,2,\cdots,|M|) \quad (15)$$

where $N(0,1)$ is Gaussian distribution with mean 0 and standard deviation 1. . is the standard deviation of the mutation operator controlled over the running of the algorithm as follows.

$$\sigma = \frac{1}{\sqrt{1 + iter}} \quad (16)$$

where *iter* is the iteration number of the algorithm.

It is worth of notice that there are no mutation probability introduced into the operation, which means that the mutation on global best position is implemented at each iteration after the global best particle is selected. It can be demonstrated by criterion of F. de Burgh that MPSO is a global convergent algorithm. The algorithm is outlined below.

MPSO-based QoS Multicast Routing Algorithm

Input: The dimension of the particles' positions (equal to the number of end nodes); Population size; Parameters of the network model.

Output: The best fitness value after MPSO executes for MAXITER iterations; optimal multicast tree.

Procedure:

1. Initialize the population;
2. **for** *iter*=1 to MAXITER
3. Compute the fitness value of each particle according to (8);
4. Update the personal best position P_i ;
5. Update the global best position P_g ;

6. Undertake the mutation operation on P_g according to formula (15) and (16);
7. **for** each particle in the population
8. Update each component of the particle's position by (6) and (7) and adjust the component t_i as an integer in $[1, n_i]$;
9. **endfor**
10. **endfor**

5. EXPERIMENT

To test the performance of the MPSO-based Multicast Routing Algorithm, we use the network model in Figure 1 as our tested problem. In the experiments, it is assumed that all the end nodes of multicast satisfy the same set of QoS constraints without regard to the characteristics of the nodes. The characteristics of the edges described by a quaternion （d, j, b, c）with the components representing delay, delay-jitter, bandwidth and cost, respectively. For performance comparison, we also used Particle Swarm Optimization (PSO) to test the problem. The experiments were realized with Visual C++6.0 on Windows XP and executed on a PC with 2.10GHz-CPU and 256MB-RAM.

The experiment configuration is as follows. The population size for PSO and MPSO is 50 and maximum number of iterations is for both algorithms and the number of the end nodes is 5. The fitness function is formula (8) with ω_1=1，ω_2=0.5，ω_3=0.5，ω_4=0.3，α=0.5，β=0.5，σ=0.5. There are 23 nodes in the network model (Figure 1), we assume node 0 to be the source node; the set of end nodes to be M={4,9,14,19,22}. The inertia weight *w* in PSO and MPSO decreases linearly from 0.9 to 0.4 over a running and acceleration coefficients c1 and c2 are fixed at 2.0.

We adopt two sets of constraints in the experiments:

1. When delay constraint D=20, delay-jitter constraint J=30，bandwidth constraint B=40 and packet loss constraint L=0.002, the multicast trees generated by the two algorithms are shown in Figure 2(a) and Figure 3(a), respectively.
2. When delay constraint D=25, delay-jitter constraint J=35 and bandwidth constraint B=40 and packet loss constraint L=0.002, the multicast trees generated by the three algorithms are shown in Figure 2(b) and Figure 3(b), respectively.

For constraints that D=25, J=35, B=40 and L=0.002, we recorded in Table 1 the dynamic changes of best fitness values when the algorithms are executing. The best fitness values generated by MPSO and PSO after 200 iterations are 0.2243225 and 0.223214. We can conclude that MPSO has the best performance and could yield better multicast tree than two other algorithm. Table 1 shows the dynamic changes of cost, delay and delay-jitter with the development of iteration for three algorithms. It can be seen that convergence speed of MPSO is more rapid than PSO. Thus it can be concluded that MPSO has stronger global search ability than PSO.

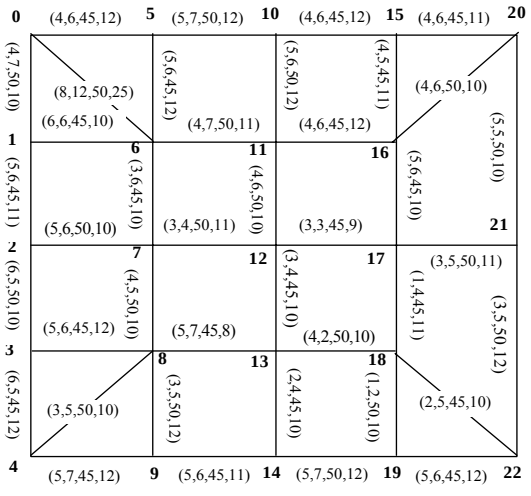
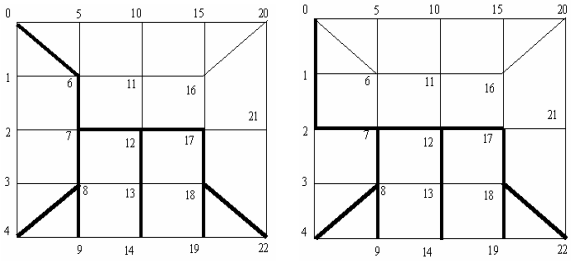
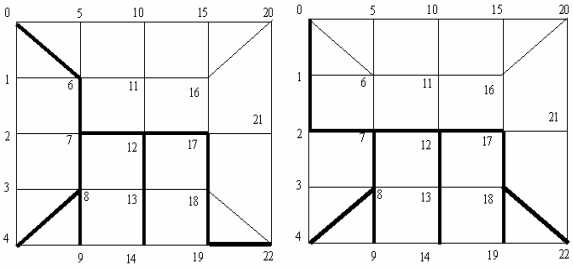


Fig.1. A network model as the testing paradigm in our experiments



(a) (b)

Fig. 2. Multicast trees generated by PSO Algorithm. (a). D=20, J=30, B=40 and L=0.002; (b). D=25, J=35, B=40 and L=0.002;



(a) (b)

Fig.3. Multicast trees generated by MPSO Algorithm. (a). D=20, J=30, B=40 and L=0.002; (b). D=25, J=35, B=40 and L=0.002;

Table 1. Dyanmic changes of best fitness values of PSO and MPSO

Iteration	PSO	MPSO
20	0.05000000	0.08759353
50	0.07684427	0.16486325
100	0.11160742	0.19532689
150	0.14648386	0.21358990
200	0.22321417	0.22432245

6. CONCLUSIONS

The paper has presented a Modified PSO (MPSO) with mutation operation on the global position of the population to solve

multicast routing policy for Internet, mobile network or other high-performance networks. This algorithm as well as original PSO provides QoS-sensitive paths in a scalable and flexible way in the networks environment. They can also optimize the network resources such as bandwidth and delay, and can converge to the optimal on near-optimal solution within few iterations. The availability and efficiency of MPSO on the problem have been verified by experiments. We also test the original PSO for performance comparison, and the experiment results show that MPSO outperforms PSO on QoS multicast routing problem.

REFERENCES

[1] F. Van den Bergh, "An Analysis of Particle Swarm Optimizers," *PhD Thesis*. University of Pretoria, Nov 2001.

[2] Moses Charikar, Joseph Naor and Baruch Schieber, "Resource optimization in QoS multicast routing of real-time multimedia," *Proc of IEEE INFOCOM.* 2000. pp. 1518-1527.

[3] Roch A. Guerin and Ariel Orda. "QoS routing in networks with inaccurate information: Theory and algorithms," *IEEE/ACM. Trans. On Networking*, No.3, Vol.7. June. 1999. pp. 350-363.

[4] Abhishek Roy, Sajal K. Das. "QM^2RP: a QoS-based mobile multicast routing protocol using multi-objective genetic algorithm," Kluwer Academic Publishers Hingham, MA, USA. May 2004, Vol. 10, pp 271-286

[5] J. Kennedy, R. C. Eberhart, "Particle Swarm Optimization," *Proc. IEEE Int'l Conference on Neural Networks, IV.* Piscataway, NJ: IEEE Service Center, 1995, pp. 1942-1948.

[6] Li Layuan. "The routing protocol for dynamic and large computer networks". *Journal of computers*, No.2, Vol.11, 1998, PP. 137-144.

[7] Y. Shi, R. C. Eberhart, "A Modified Particle Swarm," *Proc. 1998 IEEE International Conference on Evolutionary Computation*, pp. 1945-1950.

[8] B. M. Waxman. "Routing of multipoint connections" .*IEEE Journal of Selected Area in Communications*, Dec.1998, pp. 1617-1622.

A Coordination-Aware Workflow System in Virtual Enterprises

Wei Du, Wei Liu, Hanbing Yao
College of Computer Science and Technology, Wuhan University of Technology
Wuhan China 430063
Email: wliu@whut.edu.cn

ABSTRACT

This paper focuses on evolution to classical workflow that allows more flexible execution of processes while retaining its simplicity. Having modified and extended the traditional workflow philosophy, a flexible composition model that coordinates business services according to users' real-time requirements in virtual enterprise, which is called coordination-aware model (CAM), is proposed. This evolution is based on the concept of Service Oriented Architecture (SOA) with the goal of seamlessly integrating workflow systems with new required application residing in heterogeneous environment. It provides support for cooperative process management and coordination. It offers pertinent information about work progress while maintaining adequate privacy of information, and supports dynamic process definition.

Keywords: Coordination-Aware Model (CAM), Virtual Enterprise(VE), Service Oriented Service (SOA), Coordination-Aware, Flexible Workflow System

1. INTRDUCTION

Workflow is the automation of processes, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules [1]. Along with the development of Workflow technology, some deficiencies have drawn attention. Firstly in the globalization environment, enterprises are increasingly confronted with problems of change. Their business process might vary from time to time, versatile user requirements and agile response demand need distributed business services to interact and cooperate flexibly and adaptively. But most of existing workflow systems were developed to control the execution of business processes with fairly static structures. Secondly most services available on the Internet are single and simple functional units, which is called fine-grained services. Compared to such separate services is that most business processes should be implemented depending on the composition of several single web services according to the real-time demand. We called such kind of composition Coordination-aware Model (CAM) or coarse-grained services.

Present workflow system should be improved to satisfy these new and critical requirements. A middleware is required to provide dynamic integration between partners in the value chain. In this paper, we propose a model-CAM-trying to solve problems mentioned above, in which the middleware is implemented by Web service.

The remainder of the paper is organized as follows. In section 2 some related works are mentioned. Section 3 is the architecture diagram of CAM. A cooperative workflow system based on CAM is put forward. The formal concept of CAM and behaviors of it are defined, and a correlative cases are put out in section 4. In section 5 the detailed discussions are depicted. Finally the work is summed up and future work is discussed in section 6.

2. RELATED WORK

Many works address the problem of workflow flexibility and propose the solutions depending on various popular technologies. Generally there are four approaches. The first one considers the process as a resource for action [2]. The second one uses the process as a constraint for the flow of work, but it is admitted that it may change during its lifetime. The process can be dynamically adapted during its execution[3]. The third approach consists in evolving the process model itself to allow for more flexible execution. Flexibility has to be modeled and is anticipated during the process modeling step. And the last one adds flexibility in the workflow management system execution engine itself [4].

Various investigations are based on the paradigm of service activity. Via service activity states, a consumer can monitor service progress. Most approaches only support Workflow Management Coalition (WfMC)[1] specified activity states to comply with interoperation standards such as Wf-XML and Workflow Management Facility (WMF). Conventional approaches are restricted by original granularity of process definitions that is not intended for outside partners. Therefore, determining which parts of private processes should be revealed to partners is extremely difficult.

Until now, some prototypes have been implemented. eFlow[5] is a framework that supports the specification, registry, enactment, deploy and management of composite e-services, which are modeled as processes that are enacted by a service process engine. The selection of desired service[6] is according to a set of service selection rules, which are defined in a service-broker-specific language. But services registration, discovery mechanism on semantic level is not enough [7]. eSOA is an extended Service-Oriented Architecture for supporting flexible library services integration and interoperability in a large scale digital libraries environment. Although such platform solves the critical problems of single point of failure and performance bottleneck existing in the basic SOA infrastructure [8], it is hard to control the execution of composition when some exceptions occur in P2P environment [9]. Moreover, there are still some unsolved problems in the domain of P2P network itself which hinders the implement of such proposal.

In this paper, a coordination-aware model as well as semantic web are together introduced to the traditional workflow system to solve the problems mentioned in section 1 and satisfy the on-demand business pursued by enterprises and users. CAM enables a modeler to generate various levels of abstraction (granularity) of a private process flexibly and systematically. CAM can be considered a compromised solution between privacy and publicity.

* Supported by Wuhan University of Technology Fund (Xjj2005078).

3. COORDINATION-AWARE MODEL: CAM

The CAM adopts a multi-layer architecture complying with the standard SOA. The multiple layers clearly separate the infrastructure (multiple-layer virtual enterprises and web services they provided), the semantic logic (semantic layer), the coordination-aware logic (CAM layer) and the deploy logic (coordination workflow layer).

There are three charateristics in CAM. Firstly, cooperation in VE is hierarchical. Differences between cooperation across VE and in VE make it necessary to differentiate cooperation at different business layer and select different strategies and methods for each layer. Secondly, the hierarchical structure is not static but dynamic, which means partners at the same layer can freely group according to variable market goals. Even partners at one layer can join the team at another layer and cooperate with its team members. Thirdly, workshops of an enterprise at innermost layer are self-organizational. They can organize themselves to form the cooperation structure automatically in response to sub-goals, which are results of task allocation under the restriction of resources.

The coordinations among virtual enterprise entities at different layer varies in coupling tightness. Characteristics of cooperation of each layer decide that entities at outer/higher business layer are more loosely coupled than those at inner/lower layer. For example, entities at outer layer may use heterogeneous management systems to manage their production and sales processes. On the other hand, entities inside a VE may use homogeneous management systems or even share the same system. Cooperation across several layers may only require final results from cooperative partners. However, cooperation inside a layer may need not only final results but also middle data for process instance monitor, control and data audit etc.

According to the interaction in cooperation, there are two typical cooperative ways in VE, namely outsourcing and combination. If the two enterprises are coupled by outsourcing, they have little interaction during the process in which the service provider executes the task requested by the service requester. If they are organized by combinative production, interaction is very necessary during their cooperation process.

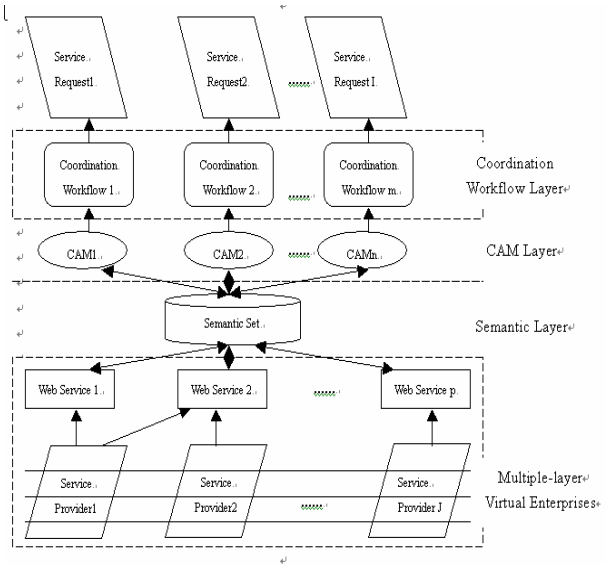


Fig.1. Coordination-aware Model

4. DEFINITIONS AND COOPERATION CONTRACTS FOR CAM

4.1 Definitions for Elements in CAM

Definition 1 (Cooperative Actor): Entities at different layer that comprise VEs are called cooperative actors denoted by ai. To meet the needs of market, ai must cooperate with each other and utilize available resources to accomplish tasks allocated according to market demands.

Definition 2 (Service): Specification which describes cooperation between cooperative actors is Service. It specifies cooperative goal, cooperative behavior, cooperative lifetime and cooperative result etc. ai. can be formally represented by a four-tuple < id, t, L, Co>

.Let id be an identifier of ai, which can specify a cooperative actor uniquely.

Let t be a task which is undertaken by cooperative actors.

Let L be a row vector denoted by [L1, L2, Li, …, Ln]. I is the number of cooperation layers of VE. L1 represents the outermost layer and Ln represents the innermost layer.

Cooperation layer moves in by from L_1 to L_m. It can be know from L the location of a_i in the cooperation by using some kind of data coding method. And values of L can be collected for analyzing cooperation states at different layer.

Let Co be a p×q matrix. P equals the number of cooperative partners and q equals the number of selected cooperative parameters. For example, let q=3. Row vector of Co is (aij, Couplingij, ServiceIDij), in which, aij is the id of the partner that cooperates with ai.; Couplingij is the coupling way between ai and aj (such as outsouring, combination, entrust and so on); ServiceIDij is the id of the service that ai and aj should comply with, which is an element in a set of sevices provided by a certain CAM.

It is defined that for any two enterprise entities, they either cooperate with each other or not. In other word, cooperation between them has two states. If there are some cooperation relationship between them, let the state value be 1. If there are not any cooperation relationship between them, let the state value be 0.

In order to describe how cooperative structure of VE changes when market objectives change, notation Pij is introduced in CAM. For certain pair entities, Pi1 describes the probability of building or remaining cooperation relationship, and Pi2 the probability of inverse state. For example, if the two entities have cooperation relationship, when they face new market requirements, the probability of remaining cooperation relationship is p11 and the probability of giving up cooperation is p12，0<p11, p12<1, p11+ p12 =1. If they do not cooperate with each other currently, when they face new market requirements, the probability of building cooperation relationship is p21 and the probabilityof keeping original state is p22，0<p21, p22<1, p21 + p22 = 1.

We can get the cooperative relation and cooperative way of VE by collecting all the four-tuples of cooperative actors and also can get the cooperative relation and cooperative way at each business layer. we also can deduce an equilibrium probability vector PT to predict the trend of cooperation way when VE facing new market wants, which is very helpful for system decision making support.

4.2 Semantics Definition in CAM

In CAM, workflows are consist of several objects and processes. In this context, a language is defined in order to describe relations between objects and processes. Along with semantic web technology, such language could improve the intellegence and flexibility of workflow system.

The notation (Object or Process)State →Transition (Object or Process) is proposed to express that a transition will depend on an object's or a process's state. The left part is a boolean expression and must be the result of ((object or process)State = = State) = true. The right part is an action that involves an object or a process in a transition. A clearest notation is : AState → Transition (B). It means that if A is in state "State", then transition will happen on B.

For example, if a process B runs when another process A will complete (i.e. such as a sequential routing), AC → Run(B) can be denoted according to the definition above. That corresponds to these properties :
1. C is a state for A object type
2. State of A is equals to Complete
3. Run is a valid transition for B object type
4. State of B is compatible to a Run transition (i.e. B is initiated, suspended, active or running and B is a process)

If all the conditions above are satisfied, B is now in running state. We are able to distinguish explicit conditions that compose a scenario and implicit ones that return exceptions. Thus, properties 1 to 3 check for inconsistency at process definition step while the later allows for capturing process errors at runtime.

4.3 Cooperation Contracts

It is easy to define cooperation between two objects. But with three or more objects, relations maybe complex and should generate more than really necessary coordination activities.

Definition 3 (object instance) : if an existing object has static attributes and dynamic behaviors an object type prossesses, such object is called object instance belonging to that object type. Assuming a represents an existing object and O (A) represents the set of corresponding object type, object instance can be denoted as a ∈ O (A) .

Definition 4 (coordination point) : The situation in which interest in two or more cooperative actors is taken inter-visibility is called coordination point. In such situation, cooperative actors exist cooperation contracts. Denote a rel b represents that a and b are cooperative actors. Denote A ∞ B represents that there is a contract exist between A and B.

When an object is involved in several relations at the same time, It should synchronize in a single coordination point or it should define two or more coordination points in order to serialize the modifications on the object.

For example, in order to perform a three-part cooperation, interest in B and C object is taken inter-visibility.

Assuming that : a ∈ O (A), b ∈ O (B), c ∈ O (C)
Then a rel b ∧ a rel c → A ∞ B ∞ C ∨ (A ∞ B) ∞ C ∨ (A ∞ B) ∞ C
Relations a rel b and a rel c mean that A and B for a part and A and C in another have accepted to share information but this is not true for B and C yet. In fact, it mean that a contract exists between A and B and another exists between A and C. That is, if those contracts include privacy protection clauses (e.g. protection of a part of a document), we must not provide entire visibility to C in B and vice versa. Thus, faced to a multi-relational description, it should test whether :
– contracts exist and allow users to share their objects in a common synchronization point. This case means that a contract also exists between B and C and allows involving A, B and C in a single synchronization point.
– contracts do not exist and we create synchronizations points for each independent cooperation.
– contracts do not exist and process participants meet for a deal. In fact, we propose new contracts.

Therefore, if a rel b, a rel c and B must process during C we are allowed to propose a global synchronization point if and only if both B and C participants accept to work together. Otherwise, we must serialize two different coordination points, selecting for example A∞B and pushing its result in a cooperation with C such as (A ∞ B) ∞ C (i.e. different from (A ∞ B ∞ C)).

4.4 A Case Study Using CAM

According to the design and definition in former sections, we take account service in bank as a simple case to study the coordination-aware model proposed in paper.

The coordination workflow based on CAM is depicted as follow Fig.2

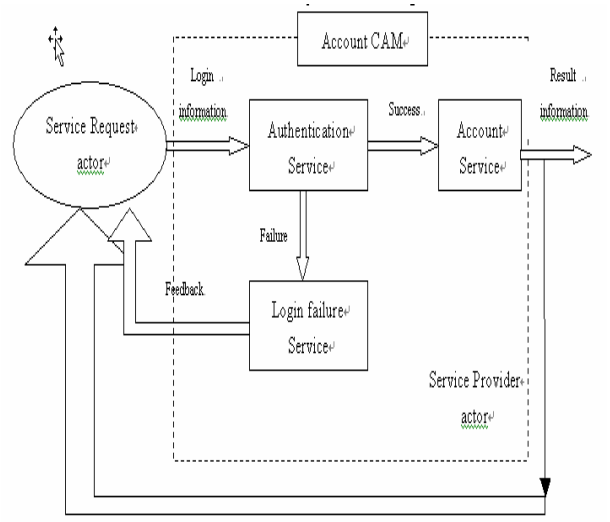


Fig.2. The Account CAM

The cooperation contract exists between two actors: servcie request actor a_1 and service provider actor a_2.

a_1 can be formally representd by $< id^1, t^1, L^1, Co^1 >$, in which:
id^1 = SR1 (i.e. Service Request actor 1)
t^1 = account request
$L^1 = (L_1, L_1)$
$Co^1 = (a12, combination, Service_3)$.
And a_2 can be formally representd by $< id^2, t^2, L^2, Co^2 >$, in which:
Id^2 = SP1 (i.e. Service Provider actor 1)
t^2 = account provider
$L^2 = (L_1, L_1)$
$Co^2 = (a_{21}, combination, Service_3)$

The critical component is Account CAM. It includes three

web services to implement account business together. The transition among them could be depicted as follow notation:

(Authentication Service)$_s$ $\rightarrow$ Run (Account Service)

(Authentication Service)$_f$ $\rightarrow$ Run (Login Failure Service)

It is also the semantic set of Account CAM. Depending on this set, CAM could provide automatic business transition in a workflow system.

The cooperation contracts between a_1 and a_2 could be represented as follow:

$a_1 \in O(SR)$, $a_2 \in O(SP)$, $a \text{ rel } b \rightarrow SR \propto SP$

5. CONCLUSIONS AND FUTURE WORK

Gartner predicted recently that by 2008, more than 60 percent of enterprises will use SOA as a "guiding principle" when creating miss-critical applications and processes. SOA represents a way to achieve a vision of seamlessly composing and interoperating between services. It is particularly applicable when multiple applications running on varied technologies and platforms need to communicate with each other [10].

Then, it will adopt a service-oriented architecture, and we rely on standards such as SOAP, WSDL and XML. This allows for accommodating both the architecture and the model without to throw away all the work ever done from future enhancements.

CAM amalgamates the mature and open technologies to improve the flexibility of traditional workflow system, which guarantee the applicability, stability and scalability. However, there are still some unsolved problems in semantic web, such as accurate description of complex business processes by structured language, the human-like intelligence of semantic web and so on. Furthermore, the implementations of QoS and cooperative transaction are deserved more detail research, especially with the number of services growing larger on the Internet. These problems are deserved more research to improve the performance of CAM.

REFERENCES

[1] Workflow Management Coalition，WfMC-TC00-1003 1996, Reference model and API specification.

[2] Nektarios Gioldasis,Nektarios Moumoutzis, etc. A Service Oriented Architecture for Managing Operational Strategies,ICWS-Europe 2003.

[3] Suchmann, L.A., Plans and Situated Action.The Problem of Human-Machine Communication, in Cambridge University Press,1987.

[4] Daniela Grigori, Francois Charoy, and Claude Godart. Anticipation to Enhance Flexibility of Workflow Execution, DEXA 2001.

[5] Fabio Casati, Ski Ilnicki, etc,Adaptive and Dynamic Service Composition in eFlow.

[6] Shuiguang Deng, Zhaohui Wu, etc,"Management of Serviceflow in a Flexible Way,"in Fifth International Conference on Web Information System Engineering, WISE 2004.

[7] Q. Chen, U. Dayal, M. Hsu and M. Griss,"Dynamic Agents, Workflow and XML for electronic Commerce Automation,"in First International Conference on E-Commerce and Web-Technology (EC'2000), UK, 2000.

[8] Zhang, Y., Shi, M. L., Miao, C.Y., et al,"Workflow Interoperability--Enabling E-Business,"in Proceedings of the Sixth International Conference on Computer Supported Cooperative Work in Design, London, Ontario (2001)

[9] U. Dayal, M. Hsu and R. Ladin,"Business Process Coordination: State of the Art, Trends, and Open Issues," In VLDB 2001, Proceedings of 27th International Conference on Very Large Data Bases, Sep, pp11–14, 2001, Roma, Italy.

[10] Papazoglou,M.P. Service-oriented computing: Concepts, characteristics and directions,WISE2003.

[11] Members., D.S.C. Owl-s 1.0 realease.

[12] http://www.daml.org/services/owl-s/1.0.(2003,Last visit: March 27, 2005)

[13] Ali Arsanjani, Service-oriented Modeling and Architecture, http://www.ibm.com.

[14] The Enterprise Service Bus.

[15] http://www-306.ibm.com/software/infol/websphere.

Crisis Management Simulation of Public Health Accident Based on Evolutionary Game Theory

Lei Yu, Huifeng Xue
Institute of Resources and Environmental Information Engineering,
Northwestern Polytechnical University, Xi'an, Shaanxi, 710072
Email: yul525@163.com

ABSTRACT

Based on the theory of Complexity Adaptive System, we attempt to study the crisis management system of public health accident through evolutionary game theory and simulate the evolutionary game through SWARM tool. Evolutionary game theory is based on bounded rationality, takes the community as the research object, and it provides the decision-making basis to the crisis management system of public health accident.

Keywords: Public Health Accident, Crisis Management, Evolutionary Game, Complexity Adaptive System, Computer Simulation

1. INTRODUCTION

In our country the public health accidents occur frequently in recent years, such as the SARS crisis and Avian Influenza. The SARS crisis lasted approximately 8 month-long has brought huge disaster and losses to our country. From global viewing, the public health accident is nearly inevitable. So establishing the mechanism to public health accident effectively has become the common duty to various countries. The public health accident process is the process of crisis management.

Because the public health accident has the characteristics of sudden, unexpected and information incomplete, crisis manager and ordinary people all have limited rationality, study of crisis management using traditional Evolutionary Game Theory has many limitations.

We attempt to study the emergency management system of public health through evolutionary game theory and simulate the evolutionary game through SWARM tool. Evolutionary game theory is based on bounded rationality, takes the community as the research object, and it provides the decision-making basis to the emergency management system of public health.

2. EVOLUTIONARY GAME THEORY

Evolutionary game theory has been well developed as an interdisciplinary science by researchers from biology, economics, social science, computer science for several decades. In past few years, it also gained the interests of physicists to study some phenomena and intriguing mechanisms in well-mixed population by using mean-field theory of statistical physics. [1]

In classical game theory, the players are assumed to be completely rational and try to maximize their utilities according to opponents' strategies. The Prisoner's Dilemma (PD) is the archetype model of reciprocal altruism. In the game, each player has two options: to defect, or to cooperate. The defector will always have the highest reward T (temptation to defect) when playing against the cooperator which will receive the lowest payoff S (sucker value). If both cooperate they will receive a payoff R (reward for cooperation), and if both defect they will receive a payoff P (punishment). Moreover, these four payoffs satisfy the following inequalities:

$$T > R > P$$

As a result, it is best to defect regardless of the co-player's decision. Thus, defection is the evolutionarily stable strategy (ESS), even though all individuals would be better off if they cooperated. Thereby this creates the social dilemma, because when everybody defects, the mean population payoff is lower than that when everybody cooperates. However, cooperation is ubiquitous in natural systems from cellular organisms to mammals. In the past two decades, some extensions on PD game have been considered to elucidate the underlying mechanisms boosting cooperation behaviors by which this dilemma could be resolved. [2,3]

This situation, however, creates a dilemma for intelligent players. They know that mutual cooperation results in a higher income for both of them. The question is then under which conditions cooperation emerges in this game.

They considered a deterministic cellular automaton where agents are placed in a square lattice with self, nearest and next-nearest interaction. At each round of the game, the payoff of the player is the sum of the payoffs she got in her encounters with her neighbors. The state of the next generation is defined occupying the site of the lattice with the players having the highest score among the previous owner and the immediate neighbors. It was remarkable the fact that within these simple rules, for a certain range of values of the pay-off matrix, very complex spatial patterns show -up with cooperators and defectors coexisting. Since then, the game has been largely extended or modified to study more complex situations.[4-6]

3. DESCRIPTION OF THE MODEL

3.1 Environment Description

The model comprises a population of agents, and an environment in which they are situated. The environment is simply a grid of cells, with each edge of the grid wrapped around to meet its opposite edge, thus forming a torus. Each cell is capable of housing any number of agents from zero upwards. Cells are used as the local area of interaction, i.e. agents can only play the PD with, and mate with, agents in the cell they currently inhabit. At each time step, agents are able to move to any of the eight adjacent cells with a certain probability.

3.2 Agent Description

Each agent is defined as having a chromosome, an energy level, and a memory of PD interactions with other agents. For every other "opponent" that an agent has interacted with during its lifetime the agent remembers both the last actions of itself and its "opponent" (cooperate (C) or defect (D) in each case). This memory is used to determine the action an agent will take next

time it meets the same "opponent". The mapping of this interaction history to an action is achieved by the agent's strategy chromosome.

The agents' chromosomes specify characteristics of the agents, and are used during interaction and mating. These chromosomes are based on (Holland 1975)'s pioneering work using genetic algorithms in adaptive artificial systems.

The genetic algorithms that we implemented in the 'ModelSwarm' consists of a canonical fitness-proportional selection scheme. Three different recombination operators were implemented: single-point crossover, two-point crossover and uniform crossover. Because we are mainly interested in the relative performance of the agents, the raw fitness *fi* (the average payoff over all played rounds) is normalized by taking $\hat{f}_i = (fi-u)/\delta+1$, where u is the mean population fitness (with standard deviation δ). This implies that a player performing one standard deviation above the mean will (on average) get two offspring. Negative and very low fitness values ($\hat{f}_i < 0.1$) were reset to 0.1 so that individuals with a very low fitness still have some (small) chance of reproducing.

The agents also have an energy level, initialized at their "birth" and decreased by a certain amount every time step. Agents "die" when their energy level reaches zero, and the only way to replenish this energy and thus survive longer is by receiving payoffs from PD interactions with other agents. The PD payoffs used were temptation $T = 5$, reward $R = 3$, punishment $P = 1$ and sucker's payoff $S = 0$.

3.3 Model Operation

An initial population is created, and randomly distributed over the environment. Each agent's initial energy level is set to a specified level. Each agent's energy level is decreased by the "living cost" specified. Any agent whose energy level reaches zero is removed from the population. All the agents move to an adjacent cell with a certain probability. Next, agents are randomly paired up within each cell, and each pair plays one round of the Prisoner's Dilemma. The action each agent chooses will be determined by their interaction history together, and their individual strategy chromosomes. As a result of this, agents' energy levels are increased in the next stage by the payoff received from the PD interaction. Finally the agents in a cell are again randomly paired.

4. PROCESS OF SIMULATION

4.1 Emergency Management System of Public Health Simulation PD Game Analysis

Fig. 1 shows Prisoner's Dilemma game simulation when $R<T$ and $S<P$ circumstances. When crisis occurred, the payoff of taking positive control strategies is higher than taking negative coping strategies regardless of whether another has positive control strategies. From fig 1 we can see that the limited rationality agents tend to take negative coping strategies over a long period of repeated PD Game.

This is because there are two balanced Game *(R, R), (P, P). (R, R)* is superior to *(P, P)* in Pareto significance. Crisis managers taking active control strategy have to pay higher costs, and negative coping strategy's costs are relatively low. This results that negative coping payoff is lower than passive control payoff. Thus, the dominant and aggressive prevention strategies of every crisis manager are waiting for others' efforts. PD Game results that both *A* and *B* choose negative coping strategy, *(P, P)* become the only game in Nash equilibrium.

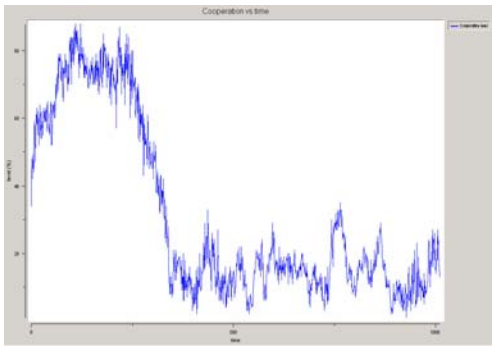


Fig.1. PD game when $R<T$ and $S<P$

4.2 Solution to Prisoner's Dilemma of Crisis Manager

To solute the Prisoner's Dilemma, it is necessary to make crisis managers who take active control strategies can get higher payoff, that is $R>T$ and $S>P$. Fig 2 shows the Prisoner's Dilemma Game analysis when $R>T$ and $S>P$. When crisis occurred, the payoff of taking positive control strategies is higher than taking negative coping strategies regardless of whether another has positive control strategies. Total PD game plans can be seen through the evolution of the results: PD game repeatedly over a long period of bounded rationality of the respondents tends to take active control strategies.

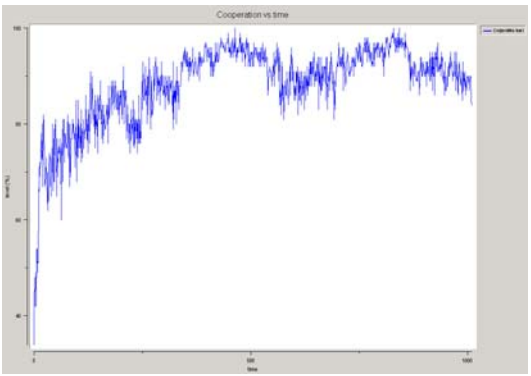


Fig. 2. PD game when R<T and S<P

5. CONCLUSIONS

Based on the theory of Complexity Adaptive System, we attempt to study the emergency management system of public health through evolutionary game theory and simulate the evolutionary game through SWARM tool. Based on the simulation results of this model, we carry on the data analysis of the solution to the Prisoner's Dilemma game of emergency manager and provide the policy suggest.

In this paper, we carried on a simple comparative analysis through the experimental results of the simulation model, and we also provided data analysis for crisis manager's PD Game solution when the public health accident approaches. We must bring the manager's employment system reform into institutionalized track. The key is adjusting the government's position, reforming the government's performance appraisal system. On the basis of the evaluation, we should establish and improve the mechanism of incentives and penalties. Spirit award is not only promotions or incentives, but also could be

considered material and other incentives. Punishment should not only be dismissed, removed, be punished in accordance with law. The purpose of this system is to improve the situation in the game to pay government officials to break the deadlock in the Prisoner's Dilemma. Officials strive to promote the public interest.

Based on the simulation results of this model, we carry on the data analysis of the solution to the prisoner's dilemma of emergency manager and provide the policy suggest. And this can avoid the emergency managers' boundedly rationality which results to collective's non-rationality and causes the crisis management to fall into the convict difficult position strange circle.

REFERFENCES

[1] Smith J Maynard,*Evolution and the theory of games[M]. Cambridge*,Cambridge University Press, 1982

[2] Weibull J,*Evolutionary Game Theory[M]*,Cambridge: MIT Press, 1995

[3] Marshall, J. A. R. S. Tokumine,"See How She Runs: Towards Visualising Artificial Red Queen Evolution,"in Jordan Pollack, Mark Bedau, Phil Husbands, Takashi Ikegami and Richard,*A. Watson. Artificial Life IX: Proceedings of the Ninth International Conference*, pp334-339 (MIT Press) , 2004.

[4] Marshall, J. A. R. J. E. Rowe,"Viscous Populations and Their Support for Reciprocal Cooperation,"*Artificial Life* 2003(9): 3, pp327-334.

[5] Marshall, J. A. R. J. E. Rowe. Kin,"Selection May Inhibit the Evolution of Reciprocation,"*Journal of Theoretical Biology,* 2003(222), pp331-335

[6] Marshall, J. A. R, J. E. Rowe,"Investigating the Mechanisms Underlying Cooperation in Viscous Population Multi-Agent Systems,"in Mark A. Bedau, John S. McCaskill, Norman H. Packard, and Steen Rasmussen (eds.) *Artificial Life VII: Proceedings of the Seventh International Conference*,pp348-352(MIT Press, 2000).

A Method of Probabilistic Logic Reasoning on Bayesian Networks*

Yong Li [1,2], Weiyi Liu [2]
[1] Department of Automation, Faculty of Information Engineering and Automation
Kunming University of Science and Technology, Kunming, 650051, China
[2] Department of Computer Science and Engineering, School of Information Science and Engineering
Yunnan University, Kunming, 650091, China
Email: leon@people.com.cn, liuweiyi2000@yahoo.com.cn

ABSTRACT

In making inferences from conditional probability information, there are critical problems. One of them is a discrepancy between logic and probability. Another is highly complex implementation calculation of higher-order logics. We propose and implement a Bayesian probabilistic logic reasoning approach, which combines Conditional Event Algebra and Markov Chain Monte Carlo simulating algorithm. By extending normal measurable space with conditional event, we first bring logic consistent with probability in denoting conditional probability information, and then we transform a higher-order conditional event to normal events and correspond logical combination events via Conditional Event Algebra. We use Gibbs simulation to sample the normal events to be a stationary state. By computing the quantitative values of the events, we can evaluate the quantitative value of higher-order conditional event at last. An example of application of our method shows how we make inferences from conditional probability information.

Keywords: Probabilistic Logic Reasoning, Bayesian Networks, Conditional Event Algebra, Product Space, Markov Chain Monte Carlo, Gibbs Sampler, Higher-order Conditional Event.

1. INTRODUCTION

In rule-based system, the rule base consists of a finite set Γ of, say, many rules, denoted such as "b→a", expressed in English as "if b then a" called "conditional rule" whose reliability is quantified by conditional probability P(a|b)[1]. The quantitative value of P(a|b) can be obtained by calculating values of normal events and correspond logical combination of events in a normal measurable space. The "if-then" is also modeled as Boolean element and its reliability is denoted as P(b→a). There exists basic discrepancy between P(a|b) and P(b→a):

$$P(b\rightarrow a)=P(b'\vee ba)$$
$$=1-P(b)+P(ba)$$
$$=P(a|b)+P(b')p(a'|b)\geq P(a|b), \quad (1)$$

with equality holding if and only if P(b)=1 or P(a|b) =1[2], and (.)' is the usual complementation operator.

On the other hand, how to denote complex conditional events such as "if if b_1 then $a_1$and if b_2 then a_2…then if d then c", i.e. higher-order conditional event[3], and evaluate its quantitative value are still under researching. In the Artificial Intelligence community, given a rule "if b then a", the probability of an event c under it may be denoted as P(c| (a|b)). But from Eq. (1), we know the quantitative value of P(c| (a|b)) can't be evaluated with P(c| (b'∨a)).

In this study, we propose and implement a Bayesian probabilistic logic reasoning approach, which combines Conditional Event Algebra (CEA) and Markov Chain Monte probabilistic logic reasoning approach, which combines Conditional Event Algebra (CEA) and Markov Chain Monte Carlo (MCMC) simulating algorithm, to above problems. By extending normal measurable space with conditional event, we first bring logic consistent with probability, and then we transform a higher-order conditional event to normal events and correspond logical combination events via CEA, and sample the events to be a stationary state with Gibbs sampler. By computing the quantitative values of the events, we can evaluate the quantitative value of higher-order conditional event or higher-order logics at last. Following an overview of result in this section, Section 2 introduces related work. Section 3 describes key ideas of CEA. Section 4 describes the method combines CEA and MCMC simulating algorithm to evaluate the quantitative value of higher-order conditional probability. In section 5, a general example is presented which illustrates the role using our method can play in addressing the two problems mentioned above. Section 6, here the paper is summarized and discusses the future work.

2. RELATED WORKS

Bayesian networks have been used in many different aspects of intelligent application. The representation and reasoning are universally interpreted in[4]. Schay, Adams, Calabrese, Goodman et al have constructed kinds of mathematics model about CEA. The typical model is Product Space Conditional Event Algebra (PSCEA) constructed by Goodman, Nguyen and Walker[5]. Based on PSCEA, Combining the theory of fuzzy logic with random sets, Goodman et al proposed Boolean Relational Event Algebra and Boolean Conditional Event Algebra[6,7]. Gyftodimos and Flach discussed combining Bayesian networks with higher-order data representations[3]. All of them discussed a serial of reasoning methods on conditioning in probability or higher-order logics from algebraic viewpoints. Deng Yong and Shi Wenkang introduce the main ideas about CEA, and discuss its application in data fusion[8]. But reasoning methods of higher-order conditional event are still need to be researched.

3. CONDITIONAL EVENT ALGEBRA (CEA)

CEA is a relatively new logic system that rigorously extends standard probability space to another including events that are contingent such as rules or conditionals.

Let (Ω,B,P) be a standard probability space, Ω be a sample space, B be a fixed event domain in the space, and P be certain probability measure. For x, s∈B, P have some characteristics as following [9]:

1) $P(\Phi)=0$, $P(\Omega)=1$.

2) $P(s_1\cup s_2\ldots\cup s_j\cup\ldots)=P(s_1)+P(s_2)\cdots+P(s_j)+\cdots$.

(conjunction), ∨ (disjunction) and ' (negation or complement) as in the Boolean algebra set.

* This work is supported by the Chun-Hui Projects of the Educational Department of China. No. Z2005-2-65003.

4) $(s|\Omega_0)=s$, i. e. the normal event is a special conditional event.
5) The probability measure P of all events in the set of Ω can be extended as the probability measure P_0 of conditional events inΩ_0, and $P_0((a|b))=P(a|b)$. Say, in CEA, conditional probability is the real probability measure about conditional events.
6) $(s|x)\wedge x=(s\wedge x)$ (modus ponens).

From 1) to 6) above we can see: in CEA, if rules were expressed as conditional event in algebra then the probability measure in probability theory could be extended into classic logic to measure quantitative values of rules, not only normal events. Thus, it is possible to calculate $P_0((a|b))$, and to express the probability weight of the rule "b→a". If a logic system that has extended Boolean event algebra and satisfied characteristics from 3) to 6) mentioned above, it could be called as conditional event algebra. PSCEA is just the Boolean conditional event algebra.

Given normal events a and b, constructing an extended production probability measurable space (Ω_0,B_0,P_0), $\Omega_0=\Omega\times\Omega\times\ldots$, B_0 is a Boolean algebra or σ-Algebra extended from B×B…, P_0 is probability measure in the space. So,

$$(a|b)=((a\wedge b)\times\Omega_0)\vee(b'\times(a\wedge b)\times\Omega_0)\vee(b'\times b'\times(a\wedge b)\times\Omega_0)\vee\ldots. \quad (2)$$

Given a function f: $B\times B\to B_0$, for all f are defined as

$$f(a,b)=ab\vee(b'\times ab)\vee(b'\times b'\times ab)\vee\ldots.$$

We have

$$P_0(f(a,b))=P_0(ab\vee(b'\times ab)\vee(b'\times b'\times ab)\vee\ldots.)$$
$$=P_0(ab)+P_0(b'\times ab)+P_0(b'\times b'\times ab)+\ldots$$
$$=P(ab)+P(b'\times ab)+P(b'\times b'\times ab)+\ldots$$
$$=P(ab)\sum(P(b'))^j=P(a|b),\quad j=0,1,2,\ldots. \quad (3)$$

In this way, (Ω_0,B_0,P_0) extends (Ω,B,P), and $P_0(f(a,b))=P(a|b)$. P_0 extends P. The rule "b→a" can be taken as an event f(a,b), but it is in another measurable space. Thus, using theorem of PSCEA, we can express the higher-order conditional events and estimate its quantitative value. But it is difficult[10].

4. COMBINING CONDITIONAL EVENT ALGEBRA WITH GIBBS SAMPLER TO MAKE INFERENCES FROM HIGHER-ORDER CONDITIONAL EVENT

4.1 Combining CEA With Gibbs Sampler

Gibbs sampler is a widely used MCMC method to simulate the Markov chain of the parameters' posterior distribution dynamically. Let π(x) be the target distribution of a s-dimensional random variable X, and the fully conditional distribution of a certain component x_i:

$$\pi(x_i|x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_s),\ (i=1,2,\ldots,s),$$

is given and all the other conditional distributions unknown, where $x=(x_1, x_2, \ldots, x_s)$.

Given the starting point $X^{(0)}=(x_1^{(0)},x_2^{(0)},\ldots,x_s^{(0)})$, Gibbs sampler algorithm, from k=0, iterates the following loop[11]:

Step 1. Sample $x_1^{(t+1)}$ from $\pi(x_1|x_2^{(t)},x_3^{(t)},\ldots,x_s^{(t)})$.
Step 2. Sample $x_2^{(t+1)}$ from $\pi(x_2|x_1^{(t+1)},x_3^{(t)},\ldots,x_s^{(t)})$.
...
Step s. Sample $x_s^{(t+1)}$ from $\pi(x_s|x_1^{(t+1)},x_2^{(t+1)},\ldots,x_{s-1}^{(t+1)})$.

Let t=t+1, the vectors $X^{(t+1)}=(x_1^{(t+1)},x_2^{(t+1)},\ldots,x_s^{(t+1)})$ (t=0,1,2,…) obtained by the iteration, are a realization of a Markov chain.

From what mentioned above, we can observe that Gibbs sampler is a method to estimate the value of f(θ|Y), Y is a observed sample and some partition of θ may be un-observed samples [12]. But it is not discussed how to use Gibbs sampler estimate the value of higher-order conditional events such as f(θ|Y|X).

The reasoning question about higher-order conditional event "if if b_1 then $a_1$and if b_2 then a_2…then if d then c" can be expressed as the scheme:

$$G=[(a|b)_J;(c|d)]. \quad (4)$$

The a_J, b_J, c, d in Eq. (4) are events under Boolean algebra, $(a|b)_J$ expresses $(a_j|b_j)_{j\ in\ J}$, P is a function denoted as

$$P: B\to[0,1]\ \text{(unit interval)}. \quad (5)$$

$(a|b)_J$ is a set of given rules, (c|d) is inferred conclusion from $(a|b)_J$, and $P(a|b)_J\geq t_J$, t_J in [0,1].

According to CEA, G can be denoted as a set of conjunction events [13]:

$$A(G)=\cap\{a_jb_j,a_j'b_j,b_j'\}\cap\{cd,c'd,d'\}=\{\omega_1,\ldots,\omega_{m+1}\}. \quad (6)$$

If no conjunction were null then $m=3^{card(J)+1}-1$, card(J) is dimension of J. According to Eq. (3), $G=[(a|b)_J;(c|d)]$ can be denoted as

$$f(a_j,b_j,c,d)=\vee(\omega_j),\ j\ in\ I(f). \quad (7)$$

From Eq. (7), for any event f in Boolean (A(G)), there is a uniquely determined index set I(f) in {1,…,m,m+1} determining it and correspondingly for any probability measure P: B→[0,1],

$$P(f(a_j,b_j,c,d))=\sum P(\omega_j),\ j\ in\ I(f). \quad (8)$$

with $P(\omega_j)$ are distributed as Dirichlet [14].

So, to estimate the quantitative value of higher-order conditional event scheme $G=[(a|b)_J;(c|d)]$ is equivalent to calculate the value of normal probability events and correspond joint events $\omega_1,\ldots,\omega_{m+1}$. Using Gibbs sampler to sample$\omega_1,\ldots,\omega_{m+1}$ to be a stationary state, we can obtain the quantitative value of $P((a|b)_J;(c|d))$, and finish inference of higher-order conditional event. To calculate the value of$\omega_1,\ldots,\omega_{m+1}$ need to use Bayesian networks. The following algorithm may be used to estimate the quantitative value of higher-order conditional events.

Algorithm PS-Gibbs: Given scheme $G=[(a|b)_J;(c|d)]$ and correspond Bayesian networks, calculating $P((a|b)_J;(c|d))$.

Step 1. Set higher-order conditional events as $G=[(a|b)_J;(c|d)]$.

Step 2. Using CEA change G to normal events and joint events $\omega_1,\ldots,\omega_{m+1}$:

a_jb_jcd, $a_jb_jc'd$, a_jb_jd', $a_j'b_jcd$, $a_j'b_jc'd$, $a_j'b_jd'$, $b_j'cd$, $b_j'c'd$, $b_j'd'$, $j\in J$.

Step 3. Combining Bayesian networks with Gibbs sampler to get a stationary state of $\omega_1,\ldots,\omega_{m+1}$.

Step 4. Calculating and unitizing the quantitative values of $P(\omega_1),\ldots,P(\omega_{m+1})$.

Step 5. Sum $P(\omega_1),\ldots,P(\omega_{m+1})$ and quit.

4.2 Convergence Diagnostics for PS-Gibbs

In above algorithm, step 3 is computed as following:
Scheme G can be presented as Fig.1, and its quantaitive value can be obtained by estimating correspond each branch as Fig.2.

From Fig.1, we have

$$G=[(a|b)_J;(c|d)]=a_1P((c|d)|\ a_1)\cup\ldots\cup a_jP((c|d)|\ a_j). \quad (9)$$

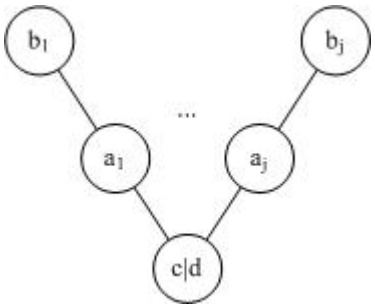


Fig.1. Structure of scheme G

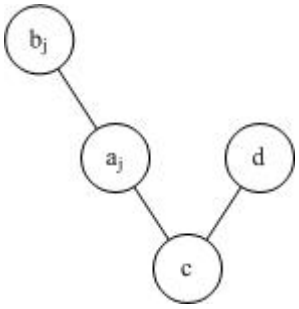


Fig.2. Structure of a branch of scheme G

According to Bayesian formula, we also have

$$a_j=b_jP(a_j\,|b_j), \quad (10)$$

and

$$G=[(a|b)_J;(c|d)]=\cup\, b_iP(a_i|\, b_i)P((c|d)|\, a_i),\ i=1,\ldots,J. \quad (11)$$

Thus, to compute the quantitative value of scheme G is transformed to calculate the value of each branch of scheme G as Fig.2 and sum all up. For

$$G_j=b_jP(a_j\,|b_j)\ P((c|d)|\, a_j), \quad (12)$$

with $P((c|d)|\, a_i)=P((c|d)|(a_j|\Omega))$.

From Eq. (7) and (8), there exists

$$P(f(a_j,c,d))=\sum P(\omega_i),\ i=1,\ldots,9, \quad (13)$$

and

$$A(G_j)=\{a_j\times\Omega,a_j'\times\Omega,\Omega'\}\cap\{cd,c'd,d'\}$$
$$=\{\omega_1,\ldots,\omega_9\}. \quad (14)$$

The Eq. (14) is just accord with Eq. (6). Based on property of Markov blankets, $P(\omega_i)$ may be calculated when a_j,b_j,c,d are sampled to be stationary.

We calculate the quantitative value of $P(\omega_1)$ as an example. From Fig.2, we have

$$P(a_j,b_j,c,d)=P(b_j)P(a_j|b_j)P(d|a_jb_j)P(c|a_jb_jd)$$
$$=P(b_j)P(a_j|b_j)P(d)P(c|a_jd). \quad (15)$$

From Eq. (15), we need to compute values of $P(b_j)$, $P(a_j|b_j)$, $P(d)$ and $P(c|a_jd)$ by Gibbs sampler combining with property Markov blankets. A Markov blanket MB[X] of a node X in a Bayesian network is any subset S(X not in S) of nodes for which X is independent of U-S-X given S and U is the set of all nodes. Pearl pointed out that in any Bayesian network, the union of the following 3 types of neighbors is sufficient for forming a Markov blanket of a node X: the direct parents of X, the direct successors of X and all direct parents of X's direct successors[4].

The convergence of algorithm PS-Gibbs is discussed as following.

Theorem 1: Using Gibbs sampler to estimate the posterior distribution of parameters $\omega_1,\ldots,\omega_{m+1}$ in Eq. (6), a stationary state of parameters can be obtained.

Proof: From analysis mentioned above, although $\omega_1,\ldots,\omega_{m+1}$ are sampled with Gibbs sampler, but eachω_i is composed of normal events and correspond joint events, say, to sample ω_i is equivalent to sample normal events and correspond joint events.

Let Q_i be the variable to be sampled and Q_{-i}' be all the variables other than Q_i. The vector q_i is the value of state Q_i and q_{-i}' is the value of state Q_{-i}'. Let $\pi_t(q)$ be probability of system in state q at point of time t, $\pi_{t+1}(q')$ be probability of system in state q'at point of time t+1 and e be evidence. When a new state q_i is sampled, we have transition probability

$$P(q\to q')=P((q_i, q_{-i}')\to(q_i', q_{-i}'))=P((q_i'|q_{-i}',e)).$$

Thus

$$\pi_t(q)\ P(q\to q')=P(q_i|e)\ P(q_i'|\ q_{-i}',e)$$
$$=(P(q_i,e)/P(e))P(q_i',q_{-i}',e)/P(q_i',e))$$
$$=(P(q_i,e)/P(e))P(q_i',e)/P(q_{-i}',e)),$$

and

$$\pi_{t+1}(q')\ P(q'\to q)=P(q_i'|e)P(q_i|\ q_{-i},e)$$
$$=(P(q_i',e)/P(e))P(q_i',q_{-i}',e)/P(q_{-i}',e))$$
$$=(P(q_i,e)/P(e))P(q_i',e)/P(q_{-i}',e)).$$

Therefore, we have

$$\pi_t(q)\ P(q\to q')=\pi_{t+1}(q')\ P(q'\to q).$$

Similarly, Markov chain is stationary.

5. AN EXAMPLE OF APPLICATION

Given events a, b, c and d described as following:
b=y means observer saw a battleship in a field.
d=y means observer saw a battleship in another field.
a=y is an observed set collected from sensors.
(a=y|b=y) means if observer saw a field in a field then sensor collect observed set a.
(c=y|(a=y|b=y),d=y) combines the experience knowledge (rule) "if observer saw a battleship in a field then sensor collect observed set" with the normal event "observer saw a battleship in a field". When computing the posterior distribution of (c=y|(a=y|b=y),d=y), it can be described as

$$P\ (c|(a|b),d). \quad (16)$$

Eq. (16) can be denoted as

$$P_0((c|\Omega)|(a|b),(d|\Omega)), \quad (17)$$

i.e. to estimate the measure weight of scheme G=[(a|b),(d|Ω), (c|Ω)].

From Eq. (6), there exists

$$A(G)=\{ad,a'd,b'\}\wedge\{d\times\Omega,d'\times\Omega,\Omega'\}\wedge\{c\times\Omega,c'\times\Omega,\Omega'\}=\{\omega_1,\ldots,\omega_{27}\}. \quad (18)$$

For $\Omega'=\Phi$, Eq. (18) is

$$A(G)=\{ad,a'd,b'\}\wedge\{d\times\Omega,d'\times\Omega\}\wedge\{c\times\Omega,c'\times\Omega\}$$
$$=\{\omega_1,\ldots,\omega_{12}\}$$
$$=\{abcd,abcd',a'bcd,a'bcd',b'cd,b'cd',abc'd,abc'd',$$
$$a'bc'd,a'bc'd',b'c'd,b'c'd'\}. \quad (19)$$

In Eq. (19), we have

$\omega_5=b'cd=ab'cd+a'b'cd,$
$\omega_6=b'cd'=ab'cd'+a'b'cd',$
$\omega_{11}=b'c'd=ab'c'd+a'b'c'd,$
$\omega_{12}=b'c'd'=ab'c'd'+a'b'c'd'.$

Given Fig.3 as following:

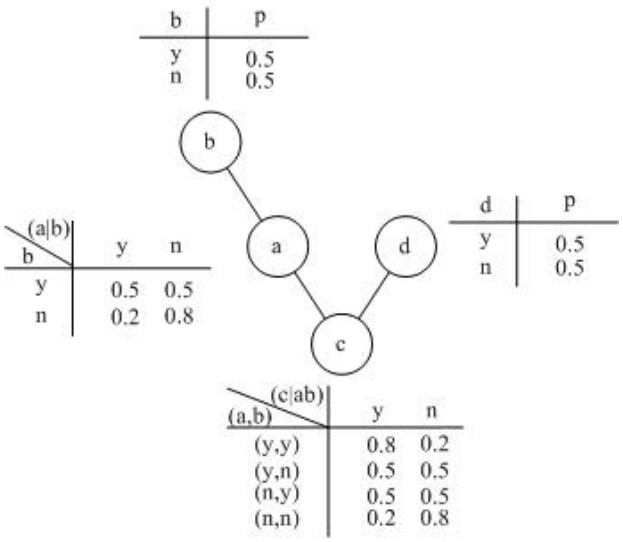


Fig.3. An example of application

From the analysis mentioned above we know that the stationary state of $\{\omega_1,\ldots,\omega_{12}\}$ needs to sample events a, b, c, d to be stationary, then calculating the quantitative values of $\omega_1,\ldots,\omega_{12}$ respectively.

Given evidence variable d=y, the initial state is {a=y, b=y, c=y, d=y}. The following steps are executed repeatedly.
1) b is sampled, given the current values of its Markov blanket variables:
P(b=y|a=y, c=y, d=y) =P(b=y)P(a=y|b=y)=0.25.
Suppose r_B=0.2 (random number), the result is b=y. Then the new state is {a=y, b=y, c=y, d=y}.
2) a is sampled, given the current values of its Markov blanket variables:
P(a=y|b=y, c=y, d=y)
=P(b=y)P(a=y|b=y)P(d=y)P(c=y|a=y, d=y)=0.1.
Suppose r_A=0.1,the result is a=y. Then the new state is {a=y, b=y, c=y, d=y}.
3) c is sampled, given the current values of its Markov blanket variables:
P(c=y|a=y, b=y,d=y)=P(d=y)P(c=y|a=y,d=y)=0.4.
Suppose r_C=0.3,the result is c=y. Then the new state is {a=y, b=y, c=y, d=y}.Then we can compute the value of $P(\omega_1)$ using P(a=y, b=y, c=y, d=y). With the different suppose value, the value of $P(\omega_i)$ can be computed.

We have implemented the PS-Gibbs algorithm with Java computer language, and time for 30000 updates on was 800MHz PentiumPro 8s. A 100 update burn in followed by a further 29900 updates gave the parameter $\{\omega_1,\ldots, \omega_{12}\}$ estimates. At last, we obtained
$P(\omega_1)$=0.66539, $P(\omega_2)$=0.00813, $P(\omega_3)$=0.00087, $P(\omega_4)$=0.00011, $P(\omega_5)$=0.08069, $P(\omega_6)$=0.00822, $P(\omega_7)$ =0.00085, $P(\omega_8)$ =0.64342, $P(\omega_9)$=0.03918, $P(\omega_{10})$ =0.07200, $P(\omega_{11})$ =0.07291, $P(\omega_{12})$ =0.40313.

By unitizing $P(\omega_1)$ to $P(\omega_{12})$, we can finally estimate P(c|(a|b),d)=0.74226. It is near to the probability of event c under events a, d in Fig.3. We give the estimated results of ω_1, ω_2, ω_3 as examples in Fig.4. X-axis denotes the iterated step, and Y-axis denotes the correspond value of $P(\omega_i)$.

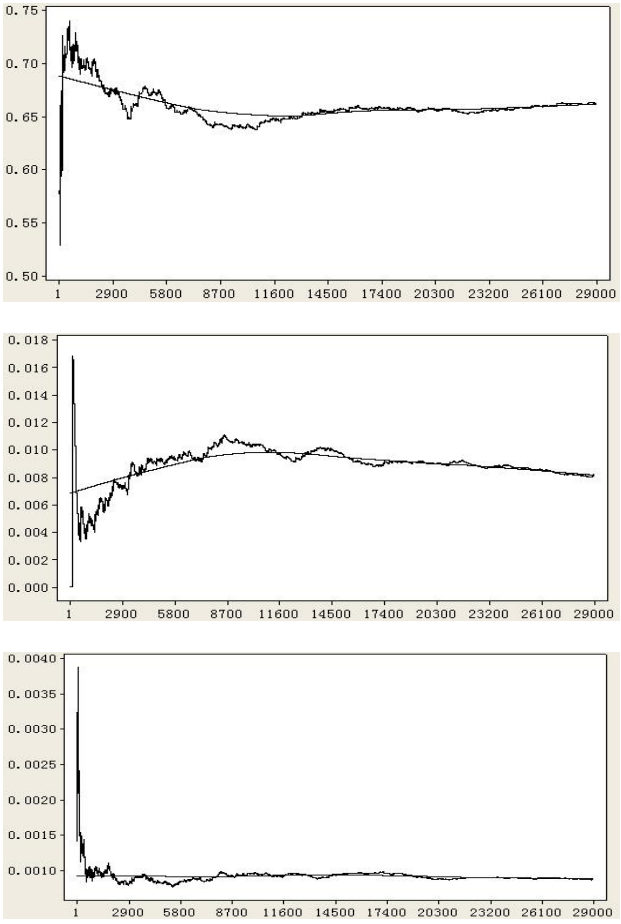


Fig.4. Statistics plots for diagnosis of convergence with parametersω_1, ω_2, ω_3

According to convergent condition of MCMC, if parameters model is convergent then the iterated results are trend to be stationary[15]. In Fig.4, the traces of 3 chains are stationary after about 20000 updates. It indicates the algorithm is convergent.

6. CONCLUSIONS

In making inferences from conditional probability information, we use CEA to resolve the problem of the discrepancy between probability and classic logic, and transform higher-order conditional event to normal events and correspond joint events. By using Gibbs sampler we obtain the normal events and joint events in a stationary state. At last, the quantitative value of higher-order conditional event is estimated. The Gibbs sampler has inner parallel characteristics[16], and using characteristics of the Dirichlet family of distribution we can estimate ω_1, …, ω_{m+1} by estimating ω_1, …, ω_m[17]. The two ways may advance the efficient of reasoning in higher-order conditional event obviously. These research issues are our future work.

REFERENCES

[1] D. Bamber, I.R. Goodman and H.T. Nguyen, "Deduction from Conditional Knowledge," *Soft Computing*, Vol.8, No.4, 2004, pp.247~255.
[2] I.R. Goodman, R.P.S. Mahler and H.T. Nguyen, *Mathematics of Data Fusion*, Kluwer Academic Publisher, 1997.

[3] Eilas Gyftodimos, Peter A. Flach, "Combining Bayesian Networks with Higher-order Data Representations," *Springer-Verlag*, A.F. Famili et al (EDs):IDA 2005, LNCS 3646, pp.145~156.
[4] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, San Mateo CA: Morgan Kaufman Publishers, 1988.
[5] I.R. Goodman, H.T. Nguyen, E.A. Walker, *Conditional Inference and Logic for Intelligent systems: A Theory of Measure-Free Conditioning*, Amsterdam: North-Holland, 1991.
[6] I.R. Goodman, G.F. Kramer, "Recent Use of Relational Event Algebra, Including Comparisons, Estimation and Deductions for Probability-functional Models," in *Proceedings of the 1998 IEEE ISIC|CIRA|ISAS Joint Conference*, Gaithersburg, September, 14-17, 1998, pp.543~548.
[7] C.T. William, D. Bamber, I.R. Goodman, H.T. Nguyen, "A New Method for Representing Linguistic Quantifications by Random Sets with Applications to Tracking and Data Fusion," *ISIF*, Vol.2, 2002, pp.1308~1315.
[8] Deng Yong, Liu Qi, Shi Wenkang, "A Review on Theory of Conditional Event Algebra," *Chinese Journal of Computer*, Vol.26,No.6, 2003, pp.650~661, China.
[9] I. R. Goodman, R. P. S. Mahler and H. T. Nguyen, "What is Conditional Event Algebra and Why should You Care?," *SPIE proceeding*, Vol.3720, 1999, pp.2~13.
[10] I.R. Goodman, "Toward a Comprehension Theory of Linguistic and Probabilistic Evidence: Two New Approaches to Conditional Event Algebra," *IEEE Transaction on Systems*, Man, and Cybernetics, Vol.24, No.12, 1994,pp.1685~1697.
[11] G.O. Roberts, S.K. Sahu, "Updating Schemes, Correlation Structure, Blocking and Parameterisation for the Gibbs Sampler," *Journal of the Royal Statistical Society*, Vol.59, 1997, pp.291~317.
[12] M. Tanner, Tools for Statistical Inference, *Method for Exploration of Posterior Distribution and Likelihood Function*, Springer－Veriag, 3rd Edition, 1996.
[13] D. Bamber, I.R. Goodman, "New Uses of Second Order Probability Techniques in Estimating Critical Probabilities in Command & Control Decision-making," in *Proceedings of the 2000 Command & Control Research & Technology Symposium*, June 26~28, 2000.
[14] I.R. Goodman, H.T. Nguyen, "Probability Updating Using Second Order Probabilities and Conditional Event Algebra," *Information Sciences*, Vol.131, No.3, Dec., 1999, pp.295~347.
[15] P.M.S. David, "Actuarial Modeling with MCMC and BUGS," *North American Actuarial Journal*, Vol.5,No.2, 2001, pp.96~125.
[16] L. Bauwens,M. Lubrano, "Bayesian Inference on GARCH Models Using the Gibbs Sampler," *Econometrics Journal*, Vol. 1,1998, pp.23~46.
[17] D. Bamber, I.R. Goodman, W.C. Torrez & H.T. Nguyen, "Complexity Reducing Algorithm for Near Optimal Fusion (CRANOF) with Application to Tracking and Information Fusion," *Signal Processing, Sensor Fusion, and Target Recognition X, SPIE*, Vol. 4380, 2001, pp. 269~280.

Yong Li is an Associate Professor in School of Information Engineering and Automation, Kunming University of Science and Technology. He is currently a Ph.D. candidate in School of Information Science and Engineering, Yunnan University. His research interests are in conditional event algebra, random sets theory and their application in data fusion systems.

Weiyi Liu graduated from Huazhong University of Science and Technology, Wuhan, China in 1976. Currently, he is a Professor in the School of Information Science and Engineering, Yunnan University, Yunnan, China. His research interests include fuzzy systems, data and knowledge engineering.

Study on Variable Weights in Fuzzy Systems and Control

Li Ding[1], Junwen Zhang[2], Pan Wang[1]
[1]School of Automation, Wuhan University of Technology Wuhan 430070)
[2]Huanggang Normal College
Email: jfpwang@tom.com

ABSTRACT

In this paper, some issues of variable weights synthesis (VWS) are discussed which focus on fuzzy systems and control. Firstly, the principles and methods of VWS (with variable elements synthesis (VES)) are analyzed in the general meaning; Some specific kinds of VWS/VES in adaptive fuzzy control are discussed; New viewpoints are presented for the VWS method of fuzzy inference.

Keywords: Variable Weights Synthesis (VWS), Variable Elements Synthesis (VES), Fuzzy Systems and Control

1. INTRODUCTION

Fuzzy control is a kind of effective control strategy with extensive applications, its great characteristics – human alike and independent of model draw on large quantity researchers and application engineers [1]. In some sense, the essence of the fuzzy control is a fuzzy multi-objective decision problem that orients dynamic systems.

In a multi-objective system, weights analysis is an important process. Recently, the issue of variable weights has caused the insistent concern of the academic community. Prof. Wang Peizhuang put forward its concept firstly [2], Prof. Li Hongxing and other researchers fulfilled a few valuable works in this field[3-5]. We have ever discussed some key issues about variable weights[6]. In this paper, some intensive researches will be carried out on VWS of fuzzy system and control.

2. SOME BASIC ISSUES OF VARIABLE WEIGHTS SYNTHESIS (VWS)

With the change of time/space and environment, the role and effect of the elements (objectives) which determine the whole system adjust dynamically. In such case, the weights are called as variable weights. Meanwhile, the decision in above case is named as variable weights synthesis (VWS).

Another similar concept is variable elements synthesis (VES).Simply speaking, variable elements synthesis refers that based on the change of both internal and external environment, elements (objectives) are variable in decision making process: some quit, and the others enter.

There is close relationship between variable weights synthesis and variable elements synthesis: as for a decision making problems with all elements or objectives (all possibly relative elements), when variable weights synthesis is applied, some objectives are eliminated if their weights are changed to be slight enough to be ignored; otherwise, some elements (objectives) need to join the decision process as their weights are changed to be considerable.

In reference [6], the author presented a few principles of VES:

(Principle 1) Beside the so called states (value of each objective), impaction of the environment should also be considered as the elements that influence the weights. Considering both internal and external factors is substantive in methodology.

（Principle 2） No great laws are available. Instead, many "small" laws act on some kinds of propositions respectively.

（Principle 3） Mathematical method is never the only tool for variable weights (We should be cautious to every analysable hypothesis on which mathematical method bases). AI and experiential method are also indispensable.

The above-mentioned principles also fit the VES. As for the origin and description of VES, there are different viewpoints. Mei Shaozhu presented that both subjectives and objectives elements decide the variation of weights, and the objective elements are only the exterior environment and time/space element(At the same time, he give a very initial technical route to determine variable weights based on fuzzy control) which can be described by the following formula[7]:

$$W = f(U, S) \tag{1}$$

Where, U is the exterior condition, S is the set of the time/space.

Li Hongxing argues that variable weights vector is decided by the Hardarmard product of constant weights vector and normalized state variable weights vector[3]:

$$W(X)=(w_1\cdot S_1(X),\ w_2\cdot S_2(X),\ldots,\ w_m\cdot S_m(X))/\sum_{j=1}^{m} w_j S_j(X) = W\circ S(X)/\sum_{j=1}^{m} w_j S_j(X) \tag{2}$$

Where, W is constant weights vector, X is objective vector, $S(X)$ is state variable weights vector that reflects the dynamical change of X.

There is another similar formula which reflects the deterministic role of constant weights vector:

$$W_{variable} = (1+\varepsilon) W_{constant} \tag{3}$$

Obviously, according to Principle 1, both the above-mentioned viewpoints have limitations. The former emphasizes the deterministic role of exterior elements, the latter only focus on the internal elements. In particular, the formula (2) has methodological mistake. From the law of quality-quantity interconversion in philosophy: When something (here we call it "object") is in the process of a certain quantitative change, the changes of weights are slight, non-essential and unobvious. At this time, the weights can be seen as constant weights. When qualitative change is happened, the original state of balance, stability and relative stillness is broken. The object has violent, essential and obvious change, the weights which reflect relative essentiality of its elements will change a lot. Therefore, the authors consider: a constant weight is only an approximation of a variable weight within a special degree, that is, a constant weight is a special result of its cause – the corresponding variable weight in corresponding degree. Obviously, a constant weight can't determine a variable weight and a variable weight can be approximated as some (even infinite) constant weights in different degrees.

3. VWS IN ADAPTIVE FUZZY CONTROL

Because fuzzy control method has the limitation of subjectivity and lacking pertinence in determining parameters and membership functions, the controlled results for complex systems are often unsatisfactory, even may be out of control. But adaptive fuzzy control (or the hybrid algorithms combing with others organically) can usually get satisfactory effect. In essence, adaptive fuzzy control can be looked as a kind of VWS and VES. Next we will discuss several adaptive fuzzy control strategies briefly.

Strategy1 [8]

$$U=\begin{cases} <c_0E+(1-c_0)EC>+U_0 & E=0 \\ <c_1E+(1-c_1)EC>+U_0 & E=\pm1 \\ <c_2E+(1-c_2)EC>+U_0 & E=\pm2 \\ <c_3E+(1-c_3)EC>+U_0 & E=\pm3 \end{cases} \tag{4}$$

Where, E, EC is the error and the error change after quantification, U and U_0 are control variable and steady state control variables respectively.

Strategy 2[1]

$$U = \frac{\beta_1|E|}{\beta_1|E|+\beta_2|EC|}E + \frac{\beta_2|EC|}{\beta_1|E|+\beta_2|EC|}EC + U_0$$
$$\beta_1+\beta_2=1;\ 0\le\beta_1,\beta_2\le1; \tag{5}$$

Where, β_1, β_2 are weighted coefficients of the control variables.

Strategy 3 [8]

$$U=\begin{cases} <c_0E>+U_0 & |E|>E_m \\ <c_1E+(1-c_1)EC>+U_0 & E_w<|E|\le E_m \\ <c_3E+(1-c_3)EC>+\beta\sum E+U_0 & |E|\le E_w \end{cases} \tag{6}$$

Where, the β is the error integral coefficient, and the E_m, E_w are thresholds From the above discussion we can know, in Strategy 1, U has the same expression but different weights of E and EC which decide the role and effect of E, EC in deciding U. More directly, the weights change with different regions of E, EC's. In Strategy 2, E, EC (internal elements) and β_1,β_2 (internal elements' weights) join the final decision process. Both Strategy 1 and Strategy 2 are VWS. In Strategy 3, the structure of expression changes with different $|E|$. Meanwhile, the corresponding weights are variable. Moreover, we can see, the less the error is (harder to control), the more complex the controller is (need to consider more elements). Obviously, Strategy 3 is both VES and VES.

4. INITIAL DISCUSSIONS ON THE VWS IN FUZZY INFERENCE

The general form of fuzzy inference is as follows:

Premise: A_{11} *and* A_{12} *and* $\cdots$ *and* $A_{1m} \to B_1$
$\cdots\ \cdots$
A_{n1} *and* A_{n2} *and* $\cdots$ *and* $A_{nm} \to B_n$

If A_1^* *and* A_2^* *and* $\cdots$ *and* A_m^*

Solute: B^*

Where, A_{ij}, A_j^* are the fuzzy sets in universe X_j; B_j, B^* are the fuzzy sets in universe Y. The solution steps are as follows [9]:

Step 1 Integrate the multiple premises into single condition. This step is called "premises reduction"

Step 2 Integrate the multiple rules into single rule. This step is called "rules reduction"

Step 3 Solute the new problem (so-called FMP).

The authors of literature [9] presented a VWS-fuzzy-inference. The key idea is to use the concept of "equipoise degree" into step 1 and 2.

As an example, consider the following VWS- Premises Reduction:

$$A_i(X) = M_m(A_{i1}(x_1), A_{i2}(x_2), \cdots, A_{im}(x_m)) = g(b(A_{i1}(x_1), A_{i2}(x_2), \cdots A_{im}(x_m)))\sum_{j=1}^{m}\omega_j A_{ij}(x_j), \tag{7}$$

$$M(X) = g(b(X))\cdot\sum_{j=1}^{m}\omega_j x_j \tag{8}$$

$$g(x) = x \tag{9}$$

Where $b(A_{i1}(x_1), A_{i2}(x_2), \cdots, A_{im}(x_m))$ is the equipoise degree of premises and ω_j is the constant weight of the i-th premise. $b(X)$ is defined as:

$$b(X) = \frac{1}{1+\sigma^2(X)} \tag{10}$$

Where,

$$\sigma^2(X) = \sum_{j=1}^{m}(x_j - \frac{1}{m}\sum_{i=1}^{m}x_i)^2$$

and

$$X = (x_1, x_2, \ldots, x_m) \in [0,1]^m$$

The above-mentioned method has several defects. Firstly, we have already illustrated in Section 2 that the variable weights can't be produced by constant weights. Above all, the above-mentioned usage of the variable weights makes mistakes in methodology. From the definition of [9], we can comprehend the authors in this literature emphasize the "equipoise" or "equipoise degree" narrowly. That is to keep each factor namely developing synchronously, going forward together, disallowing outstanding separately, this will not agree with the reasonable making decision's thought and mode – emphasizing the outstanding personality or objective. We sometimes will keep in mind specially whether to exist some special features or outstanding function objective sign (Certainly other index signs should be not very bad) Usually these special objectives decide our choice, so while making policy whether have to be balanced should deserve consideration. As the authors consider, while handling an affair, there are usually some key points (major elements), the others are secondary (minor elements), paying more attention to the main elements and considering the minor elements at the same time is the methodological demands that we have to insist on. Without majority and

minority, it will lead to neglect some important information and come to mistaken conclusions. So the real equipoise is not an absolute average and incompletely synchronous equipoise, it is the equipoise that harmonize different weighted elements, this is the right way of thinking in solving the problems of variety weights.

5. CONCLUSIONS

VWS is an important research direction of multiple disciplines. This paper discusses some issues in fuzzy systems and fuzzy control. Firstly, the principle and the processing method of VWS and VES are analyzed in the general meaning; on the aspect of adaptive fuzzy control, several kinds of VWS and VES are discussed, and in fuzzy inference, new views are put forward on how to use the VWS and VES into this field.

REFERENCES

[1] Pan Wang.,*Applicational Researches with Soft Computing for Some Decision and Control Issues*,Ph.D Dissertation. Huazhong University of Science and Technology, Wuhan, China, 2003.
[2] Peizhuang Wang,*Fuzzy Set and Projection of Stochastic Set*, Beijing: Beijing Normal University Press,1985.
[3] Hongxing Li, "Factor Spaces and Frame of Knowledge Representation(Ⅷ)– Variable Weights Analysis",in *Fuzzy Systems and Mathmatics*,Vol. 9,No.3 1995,pp.1-9.
[4] Wenqi Liu, "The Ordinary Variable Weight Principle and
[5] Multiobjective Decision-making, Systems Engineering – Theory & Practice", Vol.20, No. 3,2000,pp.1-11.
[6] Deqing Li, Cui Hongmei, LI Hongxing, "Multifactor Decision Making Based on Hierarchical Variable Weights",in *Journal of Systems Engineering*, Vol.19, No.3, 2004, pp. 258-263.
[7] Pan Wang,"Theoretical and Applicational Researches on Soft Computing Meta-synthesis,"*WHUT Technical Report* 2005-02-01, 2005.
[8] Shaozu Mei,"Fuzzy Control and the Determining of the Variable Weight,"in *Systems Engineering – Theory & Practice*,Vol.15,No.5,1996,pp.78-82.
[9] Shiyong Li,*Fuzzy Control, Neural Control and Intellgent Control Theory*,Harbin: Harbin Institute of Technology Press, 1996.
[10] Zuoyu Zhang, Hongxing Li, "A Premise Reduction Method on Fuzzy Inference Based on Variable Weights Theory, Journal of Beijing Normal University (Natural Science)", Vol.41,No.2,2005,pp.111-114.

Li Ding is a Junior student in the school of Automation , Wuhan University of Technology. His specialty is the Electrical Systems and Automation. His research interests are intelligent control, decision analysis.

Pan Wang is a Full Associate Professor and a head of Institute of Control and Decision, Wuhan University of Technology. He received the B.S. degree in industrial automation from Wuhan University of Technology, Wuhan, P. R. China, and the M.S. and Ph. D. degrees in systems engineering from Huazhong University of Science and Technology, Wuhan, P. R. China. He has published over 30 Journal papers, 20 Conference papers. He has received 10 awards of research and teaching. His research interests are intelligent control, decision analysis, and biomedical intelligent information systems.

The Application of QGA in Sensor Optimization Design *

Shijue Zheng, Xiaoyan Chen, Yanli Pei, Zhenghua Zheng
Department of Computer Science, Hua Zhong Normal University
Wuhan, Hubai, China

ABSTRACT

In this paper, the Quantum Genetic Algorithms is used to do sensor optimization design. The results indicate that the QGA can solve the problems of parameter optimization in the sensor design. The placement of sensor node is important in wireless sensor network，optimize sensor node or not ,which relate to the life circle of the network. In the past ,the algorithms be used in sensor node placement can not reach large coverage, which affect the life cycle of the network serious, researchers try many methods to solve the problem, but the result is not satisfied. With the appearance of quantum genetic algorithm, this situation has changed. In order to enlarge the coverage degree of sensor region, the paper advance quantum genetic algorithm, this algorithm use quantum bit to denote chromosome, use quantum rotation door and quantum NOT door to come true the chromosome renewal, thereby optimize the solution of the target problems.

Keywords: Wireless Sensor Networks ,Quantum Genetic Algorithm, Sensor, Node, Optimal , Placement

1. INTRODUCTION

Wireless Sensor Networks (WSNs) generally consist of a large number of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate over short distances. Their structure and characteristics depend on their electronic, mechanical and communication limitations but also on application-specific requirements. In WSNs, sensors are generally deployed randomly in the field of interest; however, there are certain applications which provide some guidelines and insights, leading to the construction of an optimal architecture in terms of network infrastructure limitations and application-specific requirements.

In sensor network, the sensor node has the end node and the route function: On one hand, realizing the data acquisition and handle, and on the other hand realizing the data anastomosing route. The number of gateway nodes is limited sometimes, and the energy can be supplied often. Gateway uses many ways to communicate with outside. But sensor node number is very ample, adopt unable complementary battery to provide an energy generally; if the sensor node energy exhausts, then the sensor node can not realize the function of data collection and routing , which have the direct impact to the entire sensor network life cycle[1].

The basic Wireless sensor network structure figure as follow:

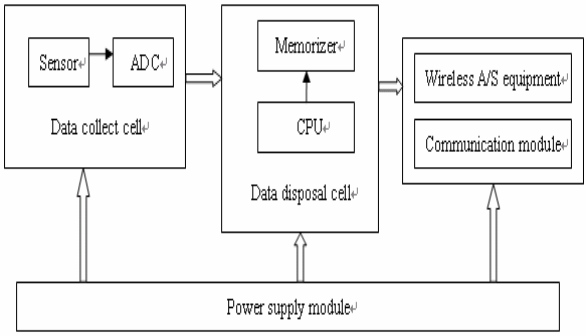


Fig.1. Structure figure

The typical composing of wireless sensor network Sensor networks play a vital role in that approach by maximizing the quantity, diversity and accuracy of information extracted from a WSN deployment. There are several sensing approaches that contribute to data collection, including remote sensing via satellites and airborne sensors, autonomous mobile systems and embedded, networked systems. WSNs belong to this last category.

2. WSN MODELING

The salient features of the proposed WSN are the following: A square grid of 30 by 30 length units is constructed and sensors are placed in all 800 junctions of the grid, so that the entire area of interest is covered. The grid is applied to open field cultivation, where a length unit is an abstract parameter so that the developed system for optimal design is general enough. The length unit is defined as the distance between the positions of two neighboring sensor nodes in the horizontal or vertical dimension. Sensors are identical and may be either active or inactive[2]. They are assumed to have power control features allowing manual or automatic adjustment of their transmit power through the base station.

2.1 Establish Target Function

The sensor node problem of this paper, how to choose a few grids to place sensor rationally. So can convert the problem to possible solution X_i(i=1,2, ,…,M)chromosome encoding to binary module: $X_i=\{b_1,b_2,\cdots,b_n\}, b_j \in \{0,1\}$

$$F(x) = f(x) + C \max\left[0, \left(\sum_{i=1}^{n} A_i B_i - K\right)\right]^2$$

Parameter as follows:

B={1,2, …n}: the grid node that can place sensor node;

U={1,2, …m}: all grid node, n<m;

Bi: decisive variable; bi=1: place sensor node in waiting location i; bi=0: do not place sensor node in waiting location i.

A_i: the cost of putting sensor in location i ($i \in B$);

K: all cost of placing sensor in monitor area;

C: gene, take arbitrarily big integers.

* This work is partially surpported by “The Theory Reseach of Architecature in Next Generation Internet”,uner Grant No.2003CB314804

2.2 The Calculation Of Fitness Value

$$f(x) = Max \frac{W_{ij}}{1 + k\sum_{k=1}^{n}(v_{ik} - v_{jk})^2}$$

W_{ij}: the distance between grid node *i* and *j*;
V_{ij}: the sensor that deployed in location *j* be able to check the target in grid node *i*; ($V_{ij}=1$, the sensor that deployed in location j be able to check the target in grid node i, $V_{ij}=0$, the sensor that deployed in location j be not able to check the target in grid node i)
V_{jk}: the sensor that deployed in location *k* be able to check the target in grid node *j*.

3. QUANTUM GENETIC ALGORITHM

Quantum genetic algorithm(QGA)[3] is the associative outcome of quantum calculation and genetic algorithm, using quantum bit encoding to denote chromosome, using quantum rotation door and quantum NOT door to come true the chromosome renewal, thereby optimize the solution of the target problems.

3.1 Quantum Bit Encoding

In QGA, the smallest unit of information is called quantum bit, which may be in the"0"state or in the"1"state, or in any superposition of the two. So a quantum bit may be in |0>、|1>, or in centre state between the both . The state of a quantum bit can be represented as $|\Psi>=\alpha|0>+\beta|1>$,where α 、β are two constant complex numbers, satisfy$|\alpha|^2+|\beta|^2=1$. $|\alpha|^2$、$|\beta|^2$are quantum bit probability in |0>、|1>state. In QGA, adopt quantum bit to denote a gene. The gene denote a certain information no longer, but contain all possible information, and any operation to the gene is able to act on all possible information at the same time. In this way, a chromosome can adopt many quantum bits to code as follows[4]:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1k} & \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2k} & \cdots & \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mk} \\ \beta_{11} & \beta_{12} & \cdots & \beta_{1k} & \beta_{21} & \beta_{22} & \cdots & \beta_{2k} & \cdots & \beta_{m1} & \beta_{m2} & \cdots & \beta_{mk} \end{pmatrix}$$

m is the number of the chromosome gene, k is the quantum bit number of every gene. α_{xy}、β_{xy} ($1\leqslant x\leqslant m$，$1\leqslant y\leqslant k$) are two constant complex number, satisfy $|\alpha_{xy}|^2+|\beta_{xy}|^2=1$.

3.2 Quantum Rotation Door

Quantum rotation door is the executive mechanism that realize the evolution operation, its adjusted operation as follows:

$$\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix} \begin{pmatrix} \alpha_i \\ \beta_i \end{pmatrix},$$

$(\alpha_i \quad \beta_i)^T$ is the chromosome before renewing ($1\leq i\leq mk$), $(\alpha_i' \quad \beta_i')^T$ is the chromosome after renewing.

Where θ_i is the rotation angle, its size and direction are ascertained by a determinate adjusted tactic. There are many adjusted tactics, a current adjusted tactic as depicted in table 1[5].

Table 1. The choice tactic of rotation angle

x_i	b_i	$f(x_i)>f(b_i)$	$\triangle\Theta_i$	$S(\alpha_i,\beta_i)$			
				$\alpha_i\beta_i>0$	$\alpha_i\beta_i<0$	$\alpha_i=0$	$\beta_i=0$
0	0	False	0	—	—	—	—
0	0	True	0	—	—	—	—
0	1	False	δ	+1	-1	0	±1
0	1	True	δ	-1	+1	±1	0
1	0	False	δ	-1	+1	±1	0
1	0	True	δ	+1	-1	0	±1
1	1	False	0	—	—	—	—
1	1	True	0	—	—	—	—

rotation angle $\Theta_i=S(\alpha i,\beta i)\triangle\Theta_i$, where $S(\alpha i,\beta i)$ is the sign of θ_i that determines the direction,$\triangle\Theta_i$ is the magnitude of rotation angle whose lookup table is shown in table1. In the Table, x_i and b_i are the *i*th measure value of current chromosome and the *i*th target value of current chromosome, respectively, $f(x_i)$ is the fitness of current measure value, $f(b_i)$ is the fitness of current target value, if $f(x_i)>f(b_i)$,adjust the corresponding quantum bit, make probability (α_i,β_i) is beneficial for b_i. In table1, δ is the angle that adjusted every time, the value of δ affect the result, if δ is too small, will affect the convergence speed; if δ is too big , it may make the result radiation, or appear the phenomenon of prematurity, the algorithm fall into local optimization. If δ is changeless, adopt the adjustment tactic of static state, or else adopt the adjustment tactic of dynamic, in which , base the difference of genetic generations, the value of δ is between $[0.005\pi,0.1\pi]$.

4. QUANTUM MUTATION

The effect of mutation is main to prevent puerile convergence and provide local searching ability. Implement mutation to chromosome: base mutation probability, exchange the location of quantum bit probability (α_i,β_i), change state "1"to state "0". To prevent the algorithm prematurity, when the best fitness value is no change in a certain algebra, implement big probability mutation to the chromosome that is in the groove, if the fitness value of the new chromosome exceed the former after mutation, so use it to replace the best fitness value of the former individual and renew the state of the chromosome.

4.1 Optimize the Placement of Sensor Node and Simulation

QGA is for optimal sensor node placement, the algorithm exceed traditional genetic algorithm (TGA)in solution. The algorithmic flow and experimental simulation as follows.
Algorithmic flow

(1) Initialize population $Q(t_0)$,in population, all genes(α_i,β_i) of entire chromosome is initialized to $(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}})$,this predict a chromosome express superposition of entire postural probability.

(2) Implement once measure to each individual in initialization population, get a set of certain solution $x(t)=\{x_1^t, x_2^t \cdots x_n^t\}$, x_j^t is the jth solution in ith population, the expressive form is binary string, whose length is m, each bit is 0 or 1. The measure step is to make a stochastic number between[0，1], if it bigger than square of probability, so measure result is 1,or is 0 .Then

make evaluation of fitness value to the solution , and record the optimal fitness individual as the target value of next evolvement.

(3) Algorithm enter to circular phase, in this phase, measure population Q(t) firstly, get a certain solution x(t), then calculate the fitness value of every solution, using quantum rotation door to adjust the individual in population, get the population Q(t+1) after renewing, reporting the current optimal solution.

(4) Compare the current optimal solution to current target value, if current optimal solution is bigger than current target value, then use the new optimal solution as the next iterative target value, otherwise, keeping current target value unchanged.

4.2 The Conditions of Convergence

QGA is a recycling searching method, it is necessary to the conditions of convergence. If the result produced by the algorithm can make the sensor node coverage all grid, algorithm end. For there is no optimal solution system, using fitness value evaluation to decide to end the algorithm or not.

4.3 Simulation Experiment

In simulation experiment, comparing TGA to QGA. Suppose monitor region is a square , acreage is 10*10, partition it to 10*10 grid, sensor nodes are deploied in the middle of the grid, Fig.2 shows the coverage degree of TGA and QGA.

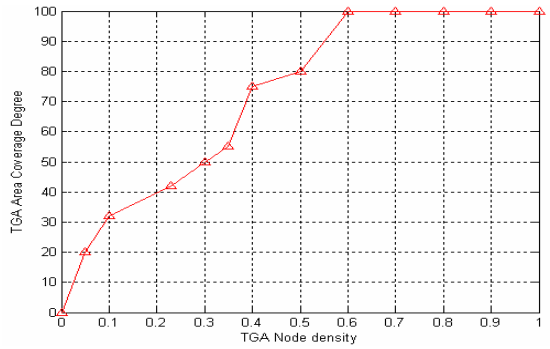


Fig.2. TGA Node density

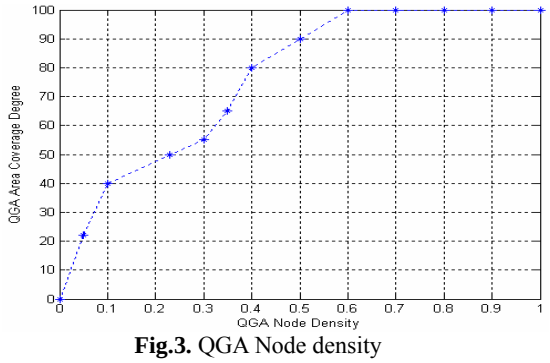


Fig.3. QGA Node density

5. CONCLUSIONS

Theoretically speaking, can adopt genetic algorithm to optimize solution, QGA has characteristics such as convergence speed quickly, calculating time shortly, getting praising highly of researcher. This paper applies quantum genetic algorithm to optimize the sensor node deployment, improving the coverage degree of sensor node, which has important influence for prolonging the life cycle of all sensor node network. In hereafter researching, will optimize quantum genetic algorithm further, making it can apply to sensor network more.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey”, *Computer Networks* 38(2002) 393–422.

[2] S.A. Aldosari, J.M.F. Moura, “Fusion in sensor networks with communication constraints”, in: *Information Processing in Sensor Networks (IPSN’04)*, Berkeley, CA, April2004.

[3] Liu Fuqiang, Zhang Lingmi. “Advances in optimal placement of actuators and sensors”.*Advances in Mechanics*, 2000, 30(4): 506-516. (in Chinese)

[4] Guo Guangcan. “Introdution to quantum information research”.*PhysicsChina*,2001,30(5):1873-1878

[5] Yang Junan, Zhuang Zhenquan. “Actuality of Research on Quantum Genetic Algorithm”, *Computer science*,2003.

Shijue Zheng, he is a professor in the Department of Computer Science,Hua Zhong Normal University.His research interests are in the field of wireless system,sensor networks and ad hoc networking.

Xiaoyan Chen was born in 1984 in Wuhan, China.She received the bachelor’s degree in 2006.She is a graduate student in Department of Computer Science,Hua Zhong Normal University.She is interested in wireless sensor network and ad hoc networking.

A New Application Area of Quantum-behaved Particle Swarm Optimization

Haiyan Lu[1], Wenbo Xu [2]
[1]School of Science, Southern Yangtze University, Wuxi Jiangsu 214122, China
[2]School of Information Technology, Southern Yangtze University, Wuxi Jiangsu 214122, China
Email:[1]helenniss2002@yahoo.com.cn,[2]xwb@sytu.edu.cn

ABSTRACT

A new method to solve nonlinear problems is proposed in this paper. Quantum-behaved Particle Swarm Optimization with random searching is used to solve nonlinear equation and nonlinear systems, which is not sensitive to initial values and does not need differential coefficient of functions. Swarm intelligence and memorial function of Particle Swarm Optimization method are used to solve sophisticated nonlinear systems. The obtained results are reported and the experiment results compared with the traditional Particle Swarm Optimization show much advantage of Quantum-behaved Particle Swarm Optimization to the traditional PSO. Conclusions are derived and directions of future research are exposed.

Keywords: Nonlinear Systems, Function Optimization, Particle Swarm Optimization (PSO), Quantum-behaved Particle Swarm Optimization (QPSO) Algorithm, Matlab

1. INTRODUCTION

Many scientific, engineering and economic problems need the optimization of a set of parameters with the aim of minimizing or maximizing the objective function.

The traditional sequential optimization methods such as Newton method, Rosenbrock method, Powell method etc., are often using a local-search algorithm that iteratively refines the solution of the problem. Unfortunately, with the extension of human activities, these traditional methods exhibited their weakness to deal with complex problems. They often fail in working upon many real-world problems that usually have a large search space, multi local optimum, and even are not well-defined. Therefore, effective optimization methods have become one of the main objectives for scientific researchers.

Modern optimization methods such as artificial neural network, genetic algorithm and ant colony algorithm etc., have shown capabilities of finding optimal solutions to many real-world complex problems within a reasonable amount of time. These methods have forged close ties with neural science, artificial intelligence, statistical mechanics, and biology evolution etc., some of them are called intelligent optimization algorithms. Recently, particle swarm optimization (PSO) algorithm has been gradually attracted more attention over another intelligent algorithm.

In the area of engineering, we often fall across nonlinear system problems. The Traditional method for solving the problems is use of initial values and the once derivation of the objective function. Sometimes it is very difficult that the initial values are suitably selected. So the traditional method can hardly detect feasible optimal solutions. In this paper, we consider to solve the nonlinear systems by Quantum-behaved Particle Swarm Optimization (QPSO) algorithm. The nonlinear systems are tackled through the minimization of a object function. In the next section, how to construct the object function is introduced. The Particle Swarm Optimization and Quantum Particle Swarm Optimization is briefly described in Section 3. The test problems and the results of experiments are reported in Section 4. The paper ends with the conclusion in Section 5.

2. FUNCTION OPTIMIZATION

It is clear that when there is an optimization problem, the goal is to find the best possible solution to the given problem. An optimization task consists of two distinct steps: creating a model of the problem and using that model to generate a solution.

In general, nonlinear equations can be described as the following nonlinear programming problem:

$$f(x)=[f_1(x), f_2(x),..., f_p(x)]^T \quad (1)$$

$a_i \le x_i \le b_i$, a_i and b_i are the search space up-bound and low-bound for x_i.

The nonlinear equations are equal to the optimization of the object function:

$$F(x)=\sum_{i=1}^{p}(f_i(x))^2, a_i \le x_i \le b_i \quad (2)$$

Traditionally, solutions to optimization problems often using either problem specific heuristics or variants of the local-search method that iteratively refines a single candidate solution to the problem. The traditional methods are not robust with respect to problem-type and often only work on well-defined problems where the number of possible solutions is not too large. The traditional methods have the unavoidable weakness that they cannot guarantee to complete their computations within a reasonable amount of time on hard and complex problems. For example, their time-complexity is exponential on NP-hard problems. We get an approximate solution to an exact model by using optimization algorithm. For practical use, optimization algorithm is often superior to the traditional methods.

3. PARTICLE SWARM OPTIMIZATION AND QUANTUM PARTICLE SWARM OPTIMIZATION

Population-based optimization algorithms have shown capabilities of approximation optimal solutions to these real-world problems within a reasonable amount of time. The best known of these algorithms is the evolutionary algorithm(EA), which is inspired by natural evolution. Furthermore, a new algorithm, the particle swarm optimization (PSO) algorithm is also a population-based search-algorithm.

3.1 Dynamics of Classical PSO

Particle Swarm Optimization (PSO)[1], originally proposed by Kennedy and Eberhart in 1995, is a population-based evolutionary, computation technique, which differs from other evolution-motivated evolutionary computation in that it is motivated from the simulation of social behavior. In a PSO system, the i th particle corresponding to individual of the organism, which depicted by its position

vector X : $x_i = (x_{i1}, x_{i2}, ..., x_{iD})$, and its velocity vector $V : v_i = (v_{i1}, v_{i2}, ..., v_{iD})$, is a candidate solution to the problem. The best previous position (the position giving the best fitness value) of the i th particle is recorded and represented as $p_i = (p_{i1}, p_{i2}, ..., p_{iD})$. The index of the best particle among all the particles in the population is represented by the symbol $p_g = (p_{g1}, p_{g2}, ..., p_{gD})$.

That is the trajectory of the particle is determined. Then the optimal solution of the probability of moving out the trajectory is ignored. Therefore, in general, PSO can obtain good solutions in high-dimensional spaces but the ignorance of optimal solution does exist and PSO stumbles on local minima.

In a classical PSO system proposed by Kennedy and Eberhart, the particles are manipulated according to the following equation:

$$v_{id}^{t+1} = \omega v_{id}^t + c_1 r_1 (p_{id}^t - x_{id}^t) + c_2 r_2 (p_{gd}^t - x_{id}^t), (d = 1, 2, ..., D) \quad (3)$$

$$x_{id}^{t+1} = x_{id}^t + v_{id}^t \quad (4)$$

$$\omega^t = (\omega^{ini} - \omega^{end})(T_{\max} - t)/T_{\max} + \omega_{end} \quad (5)$$

Where x and v denote the position and velocity of particle, i among the population correspondingly, c_1 and c_2 are two positive constants, r_1 and r_2 are two random vectors in the range [0,1]. Parameter ω is the inertia weight, which does not appear in the original version of PSO[1]. By linearly decreasing the inertia weight from a relatively large value to a small value through the course of the PSO run, the PSO tends to have more global search ability at the beginning of the run while having more local search ability near the end of the run[2,3]. In (5), t is the current step size ($t = 1, 2, ..., T_{\max}$), ω_{ini} is the initial value, ω_{end} is the ultimate value.

3.2 Dynamics of Quantum PSO

Keeping to the philosophy of PSO, a Delta Potential well model of PSO in quantum world (QPSO) [4,5,6] was proposed. Because X and V of a particle are not determined simultaneously principle, the term trajectory is meaningless in quantum world.

In Quantum-behaved Particle Swarm Optimization (QPSO), the particles move according to the following equation:

$$mbest = \frac{1}{M}\sum_{i=1}^{M} p_i = (\frac{1}{M}\sum_{i=1}^{M} p_{i1}, \frac{1}{M}\sum_{i=1}^{M} p_{i2}, ..., \frac{1}{M}\sum_{i=1}^{M} p_{id}) \quad (6)$$

$$p_{id} = \varphi * p_{id} + (1-\varphi) * p_{gd}, \varphi = rand() \quad (7)$$

$$x_{id} = p_{id} \pm \beta * | mbest_d - x_{id} | * \ln(\frac{1}{u}), u = rand() \quad (8)$$

where $mbest$ is the mean best position among the particles. φ and u are a random number distributed uniformly on [0,1] respectively and β is the only parameter in QPSO algorithm. The general QPSO algorithm is shown as follows:

1） For each particle: Initialize particle
End;
2） Calculate the value of $mbest$ by (6);
3） Calculate fitness value of each particle and its p_{id} ;
4） If the fitness value: p_{id} is better than the best fitness value in history, set current p_{id} as p_{gd} ;
5） Update p_{gd} ;
6） For each dimension of a particle, choose a stochastic number from p_{id} to p_{gd} by (7);
7） Get a new position by (8);
8） Repeat 2)~7), while maximum iterations or minimum error criteria is not attained.

4. EXPERIMENTAL RESULTS

In the experiments, we run the algorithm on Windows XP by using Matlab 7.1. The population number is 20, the maximum iteration is 3000 and the algorithm runs 50 times. The inertia weight β starting with a value close to 1.0 and linearly decreasing to 0.5 through the course of the run.

In the expressions (8), "$\pm$" is determined by the stochastic number of (0, 1). If the value>0.5, then choose "－", else choose "＋".

There are some experiments. TEST (1) and TEST (2) are nonlinear equation; TEST (3) and TEST (4) are nonlinear systems.

TEST (1):

$3x^3 - e^{\sin x} - 200 = 0$, $-100 < x < 100$

TEST(2):

$(\sin(x^3) + \cos x)e^{x^3+x+1} - 250x - \ln(x^2+1) = 0$, $-100 < x < 100$

The results for TEST (1) and TEST (2) are reported in Table 1.

Table 1. Results of two algorithms:

T=50		PSO	QPSO
(1)	x	4.0579	4.0578
	Mean of $F(x)$	0.0049	1.9853e-009
(2)	x	0.0108	0.0110
	Mean of $F(x)$	0.0327	1.0430e-006

In the case, we can see that QPSO algorithm can quickly reach the theoretical value.

TEST(3):

$$\begin{cases} (x_i - 0.1)^2 + x_{i+1} - 0.1 = 0 \\ (i = 1, 2, ..., n-1), \\ (x_n - 0.1)^2 + x_1 - 0.1 = 0 \end{cases} \quad (n = 10 , 0 \le x_i \le 10)$$

The results for TEST (3) are reported in Table 2, Fig.1, and Fig.2.

Table 2. Results of two algorithms

T=200	PSO	QPSO
x	(0.0679, 0.0671, 0.0632, 0.0627, 0.0664, 0.0629, 0.0662, 0.0645, 0.0654, 0.0670)	(0.1000, 0.1000, 0.1000, 0.1000, 0.1000, 0.1000, 0.1000, 0.1000, 0.1000, 0.1000)
Mean of F(x)	0.0388	2.5700e-010

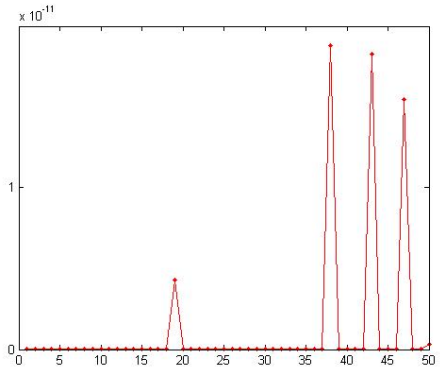


Fig.1. average of fitness curve for PSO (Iterations=1200)

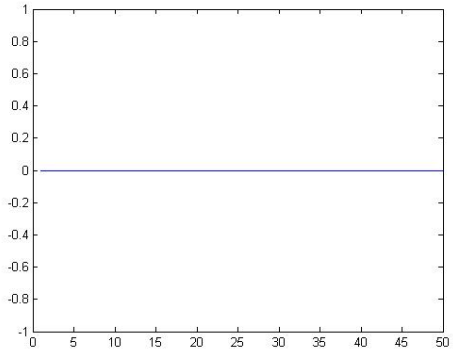


Fig.2. average of fitness curve for QPSO (Iterations=1200)

In the case QPSO outperformed the results for PSO algorithm. Especially for Fig.2 the result can reach around its theoretical value.

TEST(4):

$$\begin{cases} x_1 + \frac{1}{4}x_2^2 x_4 x_6 + 0.75 = 0 \\ x_2 + 0.405e^{(1+x_1x_2)} - 1.405 = 0 \\ x_3 - \frac{1}{2}x_4 x_6 + 1.5 = 0 \\ x_4 - 0.605e^{(1-x_3^2)} - 0.395 = 0 \\ x_5 - \frac{1}{2}x_2 x_6 + 1.5 = 0 \\ x_6 - x_1 x_5 = 0 \end{cases} \qquad -2 \le x_i \le 2$$

The theoretical value is: $\begin{cases} x_1 = -1 \\ x_2 = 1 \\ x_3 = -1 \\ x_4 = 1 \\ x_5 = -1 \\ x_6 = 1 \end{cases}$

The results for TEST (4) are reported in Table 3 and Fig.3.

Table 3. Results of two algorithms

T=3000	PSO	QPSO
x	(-1.0561, 0.2725, -0.4677, 1.3813, -1.4573, 1.4593)	(-1.0400, 0.9881, -0.9334, 1.0712, -1.0024, 1.0344)
Mean of $F(x)$	0.0521	1.0943e-004

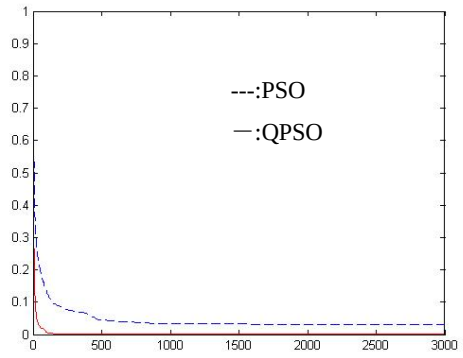


Fig.3. convergent rate of two algorithms

The results of TEST (2) show that QPSO algorithm may be even closer to its unknown theoretical value. Proper fine-tuning parameters of QPSO may result in better solutions. Fig.3 shows that for the same iterations QPSO algorithm can quickly find the answer less than 100 but PSO algorithm can not even more than 3000.

5. CONCLUSIONS

In this paper, we proposed Quantum Particle Swarm Optimization for solving nonlinear equations. According to the experimental results, the performance of the Quantum Particle Swarm Optimization method is better than PSO algorithm. QPSO algorithm can not only escape from the local minimum basin of attraction of the later phase, but also maintain the characteristic of fast speed in the early convergence phase. It has been proved that QPSO algorithm can improve the global convergence ability, greatly enhance the rate of convergence and overcome the shortcoming of PSO algorithm that is, easily plunging into the local minimum.

Future work will include investigation of the PSO's performance in other benchmark and real-life problems, as well as the development of specialized operators that will indirectly enforce feasibility of the particles and guide the swarm towards the optimum solution, as well as fine-tuning of the parameters that may result in better solutions.

REFERENCES

[1] Others: J. Kennedy and R. Eberhart, "Particle Swarm Optimization," in *Proc. IEEE Conf. On Neural Network*, 1942-1948 (1995)

[2] Shi Y, Eberhart R C, "A modified particle swarm optimizer[A]," in *Proceedings of the IEEE congress on Evolutionary Computation[C]*, Piscataway, NJ:IEEE Press, 1998. 303~308

[3] Shi Y, Eberhart R C. Empirical study of particle swarm optimization[A], in *Proceedings of the IEEE Congress on Evolutionary Computation[c]*, Piscataway, NJ:IEEE Press, 1999.1945~1950

[4] SUN J, XU WB, "A Global Search Strategy of Quantum-behaved Particle Swarm Optimization[A]," in *Proceedings of IEEE Conference on Cybemetics and Intelligent Systems[C]*, 2004.111~116.

[5] SUN J, FENG B, XU WB, "Particle Swarm Optimization with Particles Having Quantum Behavior[A],"in *Proceedings of 2004 Congress on Evolutionary Computation[C]*, 2004.325~331.

[6] Jing Liu, Jun Sun, and W.B. Xu, "Solving Constrained

Optimization Problems With Quantum Particle Swarm Optimization[A],” *DCABES and ICPACE Joint Conference on Distributed Algorithms for Science and Engineering[C]*, 2005: 99~103

Haiyan Lu (1976-) female, born in Wuxi JiangSu, China. Docent, School of Science,Southern Yangtze University. She graduated from Nanjing Normal University in 2000. Main research direction: information and computing science, evolution computing.

Wenbo Xu (1946-) Male, born in Wuxi JiangSu, China. Professor, doctor teacher, School of information technology, Southern Yangtze University, Wuxi Jiangsu, China. Main research direction: artificial intelligence, computer controlling technology, parallel computing,

The Application of RF ID and Infrared Communication Circuit to Intelligent Door Locks

Anan Fang, Xiaoli Ye, Qinwu Lai, An Zhao
Electronic Engineering Department, Nanchang University
Nanchang, Jiangxi, China
Email: Ye6d525@hotmail.com

ABSTRACT

The author introduces how RF ID intelligent door locks replace ID cards to carry out the communication and operation management of door locks. The 32-bit ARM CPU LPC2114 has been chosen as the core and real time operating system μC/OS－II as the platform to conveniently complete such functions as reading cards with RF cards, real time processing , infrared communications and operations, etc. Thus heavy desktops have been replaced. To ensure stability and reliability, proper design of circuits that enable the RF ID card data reading and ARM CPU communications is of tantamount importance.

Keywords: RF ID, ARM, CPU, LPC2114, μC/OS－II

1. INTRODUCTION

The hardware structure of RF ID intelligent door locks (See Fig.1).

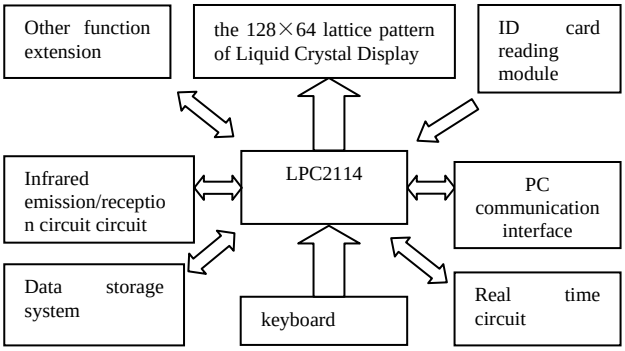


Fig.1. The Hardware Structure of Intelligent Door Locks

Its core is the PHILIPS LPC2114 chip with the ARM7TDMI－S chip as its kernel. Users are associated with other equipment through the TG1286D LCD display screen of 128×64 lattice and the 15-key keyboard. The RF ID card of the EM4100 series can be read through the ID card-reading module. The coding data is decoded by software. The data memory system uses Flash that locates in LPC2114 as its memory medium, and the real time circuit uses the low power PCF8563 clock chip. The data exchanged with the door lock can be realized through the infrared communication module. The data is modulated on the 40KHz carrier wave produced by the PWM channel of LPC2114 controlled by a kind of software. The receiver adopts the integrative receiving device and a serial interface module communicating with the upper computer is preparative. The following is a respective introduction of the principles of the hardware modules.

2. REAL TIME CLOCK CIRCUIT

PCF8563 is adopted for the real time clock chip. It is a low power CMOS real time clock/calendar chip. It provides a programmable clock output, an interruption output and power failure detector. All addresses and data transfer in series through a I^2C bus interface with the maximum bus speed of 400Kbits/s. See hardware chart: Fig. 2.

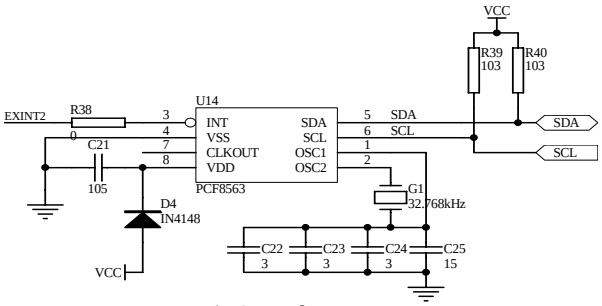


Fig.2. Real time circuit

R39 and R40 are pull-up resistors of the I^2C bus. C23～C25 are resonance capacitances of the oscillator. A reasonable combination of these capacitances can make the oscillating frequency come near 32.768KHz and achieve the highest precision of the clock. D4 is used to separate the power of the system from that of PCF8563. The electric charges stored in C21 can provide power for the clock chips during the short period of time when the handset changes its batteries, making time resetting after each battery replacement unnecessary. R38 is a zero ohm resistor, which can be soldered when needed (function extension). The interruption output connected to PCF8563 and the input of external interruption 2 of LPC2114 can realize such functions as timing start, etc.

3. RF (RADIO FREQUENCY) ID CARD READING CIRCUIT

The RF ID card reading module is divided into two parts: RF emission and reception & amplification. It is designed to be able to read the ID cards of the EM4100 series. This type of card can only be read; it can not be written. It obtains energy through the electromagnetic field generated by the card reading equipment and transfers data through the electromagnetic field. The electromagnetic wave emitting from the card and the card reading module is illustrated in Fig. 3. The emitting module circuit is illustrated in Fig. 4.

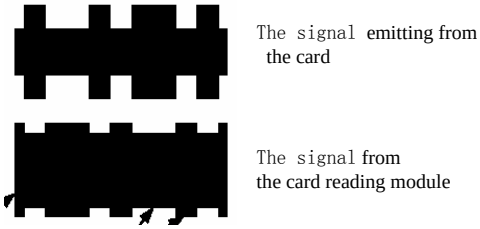


Fig.3. The electromagnetic field emitting from the card and the card reading module

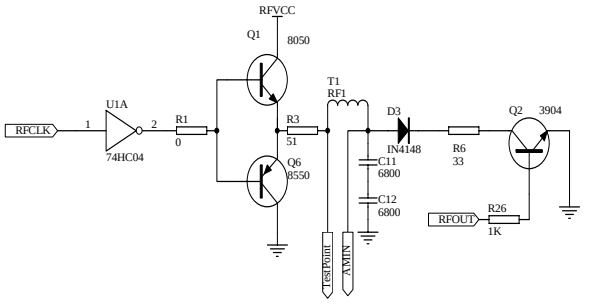


Fig.4. The emitting circuit of card reading module

74HC04 is a six-inversion-gate integrated circuit. UIA is one of the units used to reinforce the driving capability of the LPC2114 carrier wave pulse output. It transforms 0～3.3V level output from LPC2114 into the push-pull circuit following the signal driving of 0～RFVCCV. Q1 and Q6 constitute the push-pull circuit to reinforce the current load capability of the UIA output signal. T1 and C11, C12 constitute the series-wound resonance circuit, and the resonance point is the frequency needed when RF (radio frequency) ID works. The electromagnetic wave is radiated from T1. Q2 and D3, R6, R26 constitute the carrier wave amplitude modulation circuit. When RFOUT output level is high, Q2 turns on. Resonance current is absorbed partly by D3 and R6, and thus the grooves in the load wave are formed. RF (radio frequency) ID can identify the transferred data according to these grooves. Because this handset uses an ID card that cannot be written, this part of the circuit is useless. The REOUT is connected at a low level all the time.

The card reading module receiving circuit is illustrated in Fig. 5.

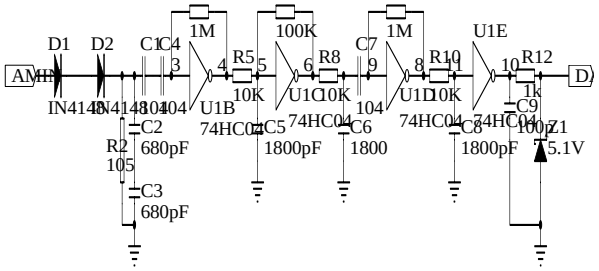


Fig.5. The card reading module receiving circuit

The voltage at one end of Loop T1 is rectified by D1 and D2. C2 and C3 filter the commutated wave, eliminating the RF part. R2 offers the discharging loop for the filtering circuit. C1 and C4 couple the signal into the following amplification circuit. The reason why the two devices are connected in series is that the voltage endurance value will be increased. There is a about 60v on AMIN, when T1and C11,C12 are in resonance. Next to the filter is the linear amplification circuit composed of U1B and R4, U1C and R7, U1D and R9. R5 and C5, R8 and C6, R10 and C8 compose first-order lowpass filter, whose edge frequency is about 8.8KHz. It can meet the need for the highest transmission speed, that being when the data cycle of the card read is at least 16 times the carrier wave cycle, 125KHz/16=7.8KHz. U1E shapes the signal amplified through three stages to make the skirt deeper so that it can be identified by LPC2114. Z1 is used to protect the I/O line of LPC2114, insuring that the receiving voltage output is not too high as to do damage to the devices. The practical effect is very good, and the card reading distance is 10cm or so.

4. THE INFRARED COMMUNICATIONS CIRCUIT

This equipment and the intelligent door lock intercommunicate through the infrared interface device connected to the Com Port 1 of LPC2114. Its carrier wave frequency is 40KHz. The principle is illustrated in Fig. 6.

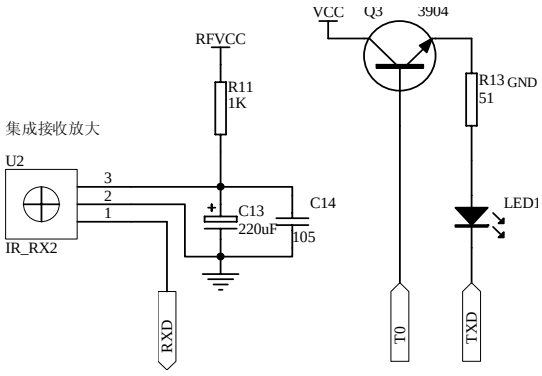


Fig.6. The infrared communications circuit

U2 is an integrative infrared receiving head, from whose first line the demodulated date is output. Q3 drives the infrared emission diode LED1. T0 is connected to the PWM channel 2 of LPC2114. Usually its output is low, but when communication with the door lock is needed, the PWM2 produces a 40KHz square wave whose filling out factor is 30% or so. TXD is connected to the transmitting terminal of the LPC2114 Com Port 1. The LED is controlled by the logical AND of T0 and TXD, producing a modulated infrared signal. RXD is connected to the receiving terminal of the LPC2114 Com Port 1. Except that the transmission medium is infrared ray, the other operations of the interface are the same as those of ordinary interfaces.

5. LIQUID CRYSTAL DISPLAY CIRCUIT

Because the equipment has much information to interact with the user, the 128×64 lattice pattern liquid crystal module is used. This kind of Liquid Crystal module is very inexpensive, but it has no word-base. Software is needed to create Chinese words, characters, cursors and graphs. The hardware chart is illustrated in Fig. 7.

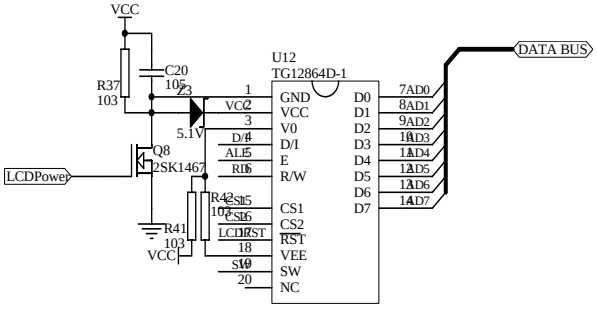


Fig.7. Liquid crystal display circuit

LCD Power line controls the turn-on and turn-off of Q8. The power of the LCD module is turned on or off through Q8 controlling its ground line. To save power, it is supplied to the LCD module only when needed. R41 and R42 constitute the voltage-divided circuit. Adjusting the differential ratio of the

divided voltages can change the display contrast. Z3 prevents the 3.3v stable-voltage chip from producing over-high voltage and doing damage to the LCD module when it breaks down. SW controls the apheliotropic lamp inside the LCD module. CS1, CS2, RAT, RW, DI and 8 data lines are used to operate each register inside the LCD module.

6. KEYBOARD CIRCUIT

This equipment has 15 key-presses, with 10 number keys and 5 function keys. The user controls the equipment through the keyboard. KEY0～KEY13 are ordinary key-presses. POWER is the system power-on /off key-press. R18～R23 and R27～R34 are the pull-up resistors of the keyboard. U3 and U4 are 8D flip-latches. LPC2114 controls the flip-latches through these three lines: CSKEY1、CSKEY2 and RDO, reading the state of the keyboard with the GPIO time-sharing. The keyboard circuit is illustrated in Fig. 8.

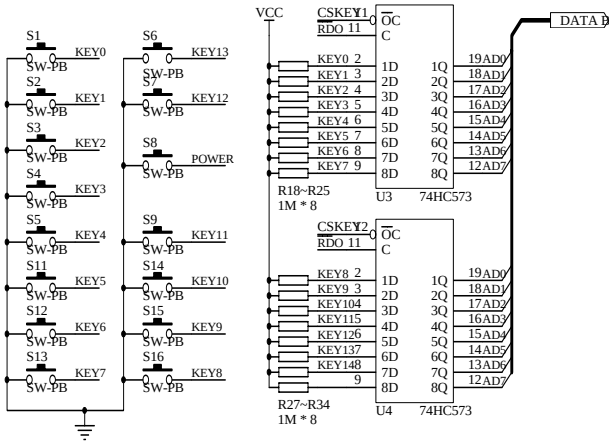


Fig.8. Keyboard circuit

The application of this equipment will make the management of the intelligent door locks easier than heretofore. It can set user cards for the door lock, synchronize the door lock time, read the door-open record and search the door-open record according to the door-open time or the card number, without the participation of an upper computer. In addition it also has the function of communicating with the upper computer to facilitate data administration.

7. THE CURRENT RESEARCH AND TRENDS AT HOME AND ABROAD

At present built-in products of low and medium complexity developed by domestic companies are mainly 8-bit micro controlled. Limited by hardware, the software is mainly the foreground and background system. In practical engineering applications the real-time operating system is seldom used. With the rapid development of semiconductor technology, presently the price of 32-bit micro controllers is close to that of 8-bit micro controllers. Yet the capability of the 8-bit micro controller is far behind that of the 32-bit micro controller.

In western countries the application of the 32-bit micro controller is not limited to the built-in applications of high complexity (such as PDA, mobile phone, Internet products etc). Its applications in the built-in systems of low and medium complexity are increasingly extensive. Because of the upgrade of hardware, the application of RTOS (real time operating system) is a necessary result. The application of built-in RTOS makes the design and extension of real time application programs easier. New functions can be added without great changes. RTOS simplifies the design process of the application programs greatly by dividing them into several independent tasks.

The ARM series 32-bit microcontrollers produced by ARM Company now occupy 80% of the 32-bit microcontroller market. They are very representative. This project is an attempt to apply the ARM 32-bit microcontrollers and the real–time operating system to the built-in systems of low and medium complexity.

REFERENCES

[1] McroC/OS Ⅱ *The Resl Time Kernel by JEAN J.LABROSSE*. [Highly Recommended] (Reviewed Dec 2000

[2] *PHILIPS Semiconductors. LPC2114/2124/2212/2214 USER MANUAL*. 2004

[3] Zhouligong “ARM Microcontrol basic and practice” *Beijing*: *The publishing company of the aviation* spaceflight University of Beijing 2003

Time-lapse Seismic Inversion Based on Parallel Simulated Annealing Using Genetic Algorithm *

Xiaohong Chen [1], Wei Zhao [1], Qicheng Liu [2]
[1]School of Natural Resources and Information Technology, China University of Petroleum
Beijing, 102249, China
[2]School of Computer Science and Technology, Yantai University
Yantai, Shangdong 264005, China
Email: ytliuqc@163.com

ABSTRACT

Parallel simulated annealing based on genetic algorithm is applied in the time-lapse seismic inversion in this paper. The seismic-derived estimates of reservoir properties estimates are often obtained from time-lapse impedance estimates, it is important to achieve reliable time-lapse impedance models through time-lapse data inversion. For solving time-lapse seismic reservoir monitoring more efficiently, simulated annealing is applied to the inversion technique of time-lapse seismic. The time-lapse seismic uses multiple seismic surveys acquired at different times, so the seismic data in the time-lapse seismic is extraordinary huge. Parallel simulated annealing based on genetic algorithm is studied in this paper; it can proceed from many points simultaneously and independently, and periodically reconcile solutions. The parallel algorithm and the parallel implements model using MPI and JINI technology is described.

Keywords: Time-Lapse Seismic, Inversion, Simulated Annealing, Parallel, Genetic Algorithm

1. INTRODUCTION

Time-lapse seismic analysis uses multiple seismic surveys (often referred to as base and monitor surveys) acquired over time. Differences in reflection amplitude and other attributes of these data vintages are interpreted and used to constrain the spatial distribution of dynamic reservoir properties and to provide insight on the depletion process. This information, when integrated with additional geological, geophysical and engineering data can invariably optimize the production strategy of the reservoir [1].

With the evolution of time-lapse seismic technologies, the industry is aiming towards seismic-derived estimates of reservoir properties that can offer more definite constraints to flow models. Since these estimates are often obtained from time-lapse impedance estimates, it is important to achieve reliable time-lapse impedance models through time-lapse data inversion.

Several researchers have reported on geophysical applications of simulated annealing method [2][3], but no researchers have introduced simulated annealing algorithm to time-lapse seismic.

For solving time-lapse seismic reservoir monitoring more efficiently, simulated annealing is applied to the inversion technique of time-lapse seismic in this paper.

* Natural Science Function of China (Grant No. 40574048) and National High Technique Scheme of China (863) (Grant No. 2006AA0AA102-09)

At the same time, with the development of oil field prospecting, more and more seismic data are produced, so parallel technology become more and more important. The time-lapse seismic uses multiple seismic surveys acquired at different times, so the seismic data in the time-lapse seismic is extraordinary huge.

Parallel simulated annealing based on genetic algorithm is studied in this paper; it can proceed from many points simultaneously and independently, and periodically reconcile solutions.

2. SIMULATED ANNEALING (SA)

SA is a robust statistical technique, which attempts to solve the problem of finding global extrema to complex optimization problems. The idea comes from the cooling processes of metals and the way, in which liquids freeze and crystallize. The basic concept of SA used in this work is as follows: each value of the model parameter is sequentially visited and randomly perturbed, while the values of all other parameters remain fixed. At each step, the change in the energy function ($\triangle E$) is calculated. The new model is accepted unconditionally if $\triangle E \leqslant 0$ (downhill moves). However, if $\triangle E > 0$ (uphill moves), then the new model is accepted according to the Boltzman probability distribution $P(\triangle E) = EXP(-\triangle E/T)$, where T is a control parameter equivalent to the temperature in annealing of crystal forming material. The entire procedure is repeated for all model parameters. Then the temperature is lowered and the procedure is repeated until "crystallization" occurs, i.e. a low energy state is attained. Thus, in SA it is still possible for a worse model to be accepted. In this way, the solution can escape from local minima. A modification of standard SA methods includes the adjustment of step length during the cooling schedule in such a way that half of the function evaluations are accepted in one direction. The decrease in step length with falling temperature allows the algorithm to focus on the most promising area and hence increases the accuracy of optimization. As the temperature falls, uphill moves are less likely to be accepted, and the percentage of rejections rises. When a set of cost function values for successive stages are less than the error tolerance for termination, the iteration process is stopped. For SA the theoretical convergence to a global minimum has been extensively proven. The system should find the global minimum if the initial temperature; the cooling rates and the number of tries are set appropriately. Ideally, starting at a high temperature and cooling very slowly guarantees convergence but it takes enormous computing time. To avoid local minima and reduce computing time, SA parameters should be defined by a trial run at the outset. Roughly, the value of the initial temperature should be of the order of the average $\triangle E$ found during the first cycle, ensuring a high accepted/rejected ratio at the start.

3. OBJECTIVE FUNCTION

Any optimization methods, whether local or global, require the construction of an objective function. Two types of objective functions are widely used in the seismic waveform inversion. One is the correlation coefficient type representing the resemblance of the observed and synthetic seismic data, which leads to a maximization problem. The other one is the least-square type showing the difference between the two, which defines a minimization problem. Ideally an objective function should contain multiple terms each representing the error energy, the low frequency component and lateral continuation constraints. The objective function used in this presentation contains a least absolute deviation, a priori parameter information constraints and a reflection coefficient penalty function. The latter means that if a reflection coefficient with unrealistically large amplitude occurs during inversion, a penalty is imposed upon the objective function. This is a particularly important constraint to ensure the smoothness of solutions when the inversion scheme is over parameterized.

4. TIME-LAPSE SEISMIC INVERSION

For the inversion of the time-lapse seismic data, we used elastic wave propagation with the following assumptions. First, the earth is assumed to be layered, i.e., the elastic parameters are functions of depth only: $V_P(z)$, $V_S(z)$, $\rho(z)$. Second, we do not model multiple reflections. Therefore, we can linearize the parameters in the wave equation (for example, $\rho(z) = \rho_0(z) + \delta\rho(z)$). Finally, the source is assumed "high frequency", and we apply geometric optics approximations. These assumptions result in the convolutional model for the seismogram:

$$d^{pred}(t, h) = f(t, h) * \check{r}(t, h) \quad (1)$$

where d^{pred} is the predicted seismic data, f the source wavelet, h is offset, and t is time. The reflectivity:

$$\check{r}(t, h) \approx (A_P(z, h)\, r_P(z) + A_S(z, h)\, r_S(z) + A_D(z, h)\, r_D(z))_{z=Z(t, h)} \quad (2)$$

where Z(t, h) is the depth corresponding to two way time t at half offset h, A_P, A_S, and A_D are geometrical amplitude factors, and P-wave velocity, S-wave velocity, and density reflectivities are

$$r_P = \delta V_P / V_P,\ r_S = \delta V_S / V_S, \text{ and } r_D = \delta\rho / \rho.$$

We use an iterative conjugate gradient algorithm to solve the discrete linear system resulting from the inversion. The objective function contains two terms. Minimize:

$$J_{OLS}[r]=0.5*\{\| d^{pred}[r]-d^{obs} \|^2+ \lambda^2 \| W[r] \|^2\} \quad (3)$$

The first term minimizes the data misfit (output least squares inversion) while the second term reduces the ill conditioning of the system.

5. PARALLEL SIMULATED ANNEALING USING GENETIC ALGORITHM

The high performance computing in the time-lapse seismic is very important; the parallel algorithm and the parallel programming model of the inversion must be studied. If given limited computational time, SA may return an unacceptable, sub-optimal solution, so we must increase the speed through parallelism.

However, because SA iterates from only one current point, it is not easily made parallel. Nevertheless, many parallel implementations have been suggested or are in use. Most suffer from the fact that they attempt to implement the inherently serial Metropolis algorithm in parallel.

A massively parallel simulated annealing would proceed from many points simultaneously and independently, and would periodically reconcile solutions. Genetic approaches attempt this, while offering the additional benefit of implicit parallelism.

5.1 Methodology

A final but important difference between genetic algorithms (GAs) and SA is the ease with which each algorithm can be made to run in parallel. GAs are naturally parallel — they iterate an entire population using a binary recombination operator (crossover) as well as a unary neighborhood operator (mutation) [4]. SA, on the other hand, iterates a single point (using only a neighborhood operator); it is not easily run on parallel processors. While attempts have been made to parallelize SA, a straightforward, satisfactory, general-purpose method has not yet been demonstrated. It would thus be desirable to transfer the parallel processing capabilities of GAs to SA.

Parallel simulated annealing based on genetic algorithm closely follows simulated annealing, if one imagines several copies of SA running in parallel, with mutation as the neighborhood operator, and crossover recombining independent solutions. Alternative solutions in parallel simulated annealing based on genetic algorithm unlike in Boltzmann tournament selection, do not come purely from the current population, but from applying both crossover and mutation. Good solutions disappear only when replaced probabilistically by new, often better solutions; disruption by crossover and mutation is not a problem.

Parallel simulated annealing based on genetic algorithm captures the essence and spirit of SA. Suppose we simultaneously run multiple, independent SAs on a problem, but we synchronize cooling across processors. This method will approach a Boltzmann distribution for each independent application of SA. The combined distribution from all applications will also approach Boltzmann. The only thing missing is to reconcile the independent solutions. This is where crossover comes in. As demonstrated later, crossover can be viewed as an extension to the common SA neighborhood operator. The resulting population-level neighborhood operator, crossover-plus-mutation, plays a role analogous to the neighborhood operator of SA.

5.2 Parallel algorithm

In the algorithm below, T is temperature, n is population size, and Ei is the energy or cost of solution i. Parameters can be set using guidelines from both SA and Gas. Parallel simulated annealing based on genetic algorithm performs minimization by default; for maximization, traditional GA fitness values should be negated.

1. Set T to a sufficiently high value
2. Initialize the population _usually randomly_
3. Repeatedly generate each new population from the current population as follows:

(1). Do n/2 times:

   a. Select two parents at random from the n population elements
   b. Generate two children using a recombination operator (such as crossover), followed by a neighborhood operator (such as mutation)

c. Hold one or two Boltzmann trials between children and parents
d. Overwrite the parents with the trial winners

(2). Periodically lower T

Boltzmann trial above mentioned refers to a competition between solutions i and j, where element i wins with logistic probability, 1/(1+e(Ei-Ej)/T) (the Metropolis criterion can be substituted). There are many such competitions possible between two children and two parents. We consider two possibilities here. The first possibility, double acceptance/rejection, allows both parents to compete as a unit against both children; the sum of the two parents' energies should be substituted for Ei in the above equation; the sum of the childrens' energies, for Ej. The second possibility, single acceptance/rejection, holds two competitions, each time pitting one child against one parent, and keeping the parent with probability, 1/(1+e(Eparent-Echild)/T). In this study, each parent is tried against the child formed from its own right-end and the other parent's left-end.

5.3 Parallel programming model

In parallel programming, there are many different languages and programming tools, each suitable for different classes of problem; our choice of tool will depend on the nature of the problem to be solved. MPI (Message Passing Interface) and Jini based on Java are particularly appropriate for the discrete wavelet parallel algorithms.

In the MPI programming model, a computation comprises one or more processes that communicate by calling library routines to send and receive messages to other processes. In most implements, a fixed set of processes is created at program initialization, and one process is created per processor. However, these processes may execute different programs [5].

The Jini programming model is built to enable services to be offered and found in the network federation. When a Jini service is developed it will have to announce its presence to other services and users. Users and services will have to discover other services and intercommunicate with them. The heart of Jini is composed of several protocols called discovery, join and lookup. The discovery occurs when a service is searching for a lookup service to register itself, the join occurs when a service has located a lookup service and wishes to join, and the lockup occurs when a service client or a user needs to locate and invoke a service.

6. CONCLUSIONS

Time-lapse seismic reservoir monitoring technique has been becoming one of the most important fields of reservoir geophysics at present. It relates with geology, geophysics, petrophysics and reservoir engineering, and realizes the conversion from static reservoir characterization to dynamic prediction and rapid reservoir evaluation, reaches the aims of adjusting development scheme and improving oil and gas recovery. A global optimization using simulated annealing and its parallelism based on genetic algorithm has been applied to the inversion technology of the time-lapse seismic. The parallel simulated annealing based on genetic algorithm strives to retain the desirable asymptotic convergence properties of simulated annealing, while adding the populations approach and recombinative power of genetic algorithms. The algorithm iterates a population of solutions rather than a single solution, employing a binary recombination operator as well as a unary neighborhood operator. The implementation of using MPI software system and JINI technology can make network parallel computing easy to implement without knowing the detail of working with a heterogeneous network of computers.

REFERENCES

[1] David E. Lumley, "Time-lapse seismic reservoir monitoring", *Geophysics,* Vol 66, pp. 50~54, 2001

[2] Goffe W. L., G. D. Ferrier, J. Rogers, "Global optimization of statistical functions with simulated annealing", J. *Econometrics,* Vol 60, pp. 65-100, 1994

[3] Sen, M.K., and Stoffa, P.L., "Nonlinear one-dimension seismic waveform inversion using simulated annealing", *Geophysics,* Vol 56, pp. 1624-1638, 1991

[4] Koza JR., "Genetic Programming: On the Programming of Computers by Natural Selection". MIT Press, 1992

[5] Bhardwaj, D., S. Phadke and Sudhakar Yerneni, "On improving performance of migration algorithms using MPI and MPI-IO". *Expanded Abstracts, Society of Exploration Geophysicists*, 2000

Xiaohong Chen is now a Professor and vice dean of School of Natural Resources and Information Technology, China University of etroleum,Beijing. He received a B.S. (1982) in Mathematics from Nanjing University, an M.S. (1988) Computational Mathematics from Harbin Institute of Technology. He received a Ph. D. (1993) in Applied Geophysics from University of Petroleum Beijing. His research interests are in information technology of seismic data processing, parallel computing.

Research and Implementation of Distributed Monitoring Systems For Power Plants

Bing Li[1], Yuhai Zhang[2], Dan Li [3]
[1]Computer College , DaQing Petroleum Institute ,Daqing 163318,China
[2]Petrochemical Company ,Chemical Plant No.2,Daqing 163714,China
[3]No.7 Division in No.1Factory of Daqing Oilfield Company Limited Daqing 163001,China
Email: lbzyh@163.com

ABSTRACT

Aiming at the comparatively laggard level of distributed monitoring systems for power plants, the reliability, real-time and several key problems of its implement are analyzed. The physical structure and logical structure of a distributed monitoring system for power plants are presented which are based on the integration of FCS (Field Bus), DCS (Decentralized Control System) and so on. Furthermore the realization methods and function characteristics of the system are expounded. Then OPC (OLE of Process Control) technology is introduced, which is important to implement the integration of electrical automation systems and management information systems. New idea employing OPC service gates is proposed. In the system, OPC service gates are responsible for the transmission of real-time data and the communication interface of field control layer and management information layer. Referring to the project experience, some technology problems, solutions and detailed schemes are discussed. The results of field applications show that the novel distributed monitoring systems have good capability, reliability and reliability.

Keywords: Power Plant, Distributed Monitoring System, OPC Service Gate, TCP/IP

1. INTRODUCTION

1) With the development of power plant technology, the requirements for distributed monitoring systems for power plants also rise [1][2]. Over the last decade, integrated automation technology has been applied in power system substation, and DCS (Decentralized Control System) and FCS (Field bus Control System) is widely used in integrated automation systems [3]. Compared to the centralized monitoring systems, distributed monitoring systems have many advantages such as flexible structure, distributed control, high reliability and so on. Instead of these advantages, distributed monitoring systems have not been widely employed in power plants. Many electrical systems and devices including protective relay, security devices and so on run in self-governed state, which haven't formed an integrated to provide information for the whole distributed monitoring system. The paper proposes a distributed monitoring system model for power plants, which is based on integrated automatic power electronic technology including real-time control, field-bus, industrial Ethernet and so on. The advantages of the system model are as follows:
2) High real-time character. Instead of traditional passive broadcast method, P2P connection method based on improved TCP/IP technology, logical token-based ring and so on guarantee the system to achieve high real-time.
3) Uniform format. In the system, all kinds of equipments are endowed with uniform IP address. Clients in management layer can transparently access the equipments by OPC service gates, which provide NAT (Net Address Transform) to equipments that have no IP addresses.
4) Centralized information and distributed control. In the system model, FCS and DCS are utilized to realize distributed control for power plant field. And OPC service gates and real-time databases are responsible for real-time and exact data such as voltage, current and so on.
5) Friendly user interface. On-line and off-line are storaged in real-time databases and history databases. With the Internet explorer, client application interfaces and others, the managers of power plants can view all kinds of information.

2. SYSTEM OBJECT MODEL

The system model discussed in the paper is referred to two types: system physical model and system logical model. And they are discussed as follows.

2.1 System Physical Model

The system physical model in the paper consists of all kinds of hard devices such as protection, measurement, control, monitoring devices, industrial personal computers (IPC) and programmable logic controller (PLC). In the subsection, the system physical model of distributed monitoring systems for power plants is proposed. And these devices and equipments are regarded as three-layer structure as follows. And Fig.1 illustrates the system physical model.

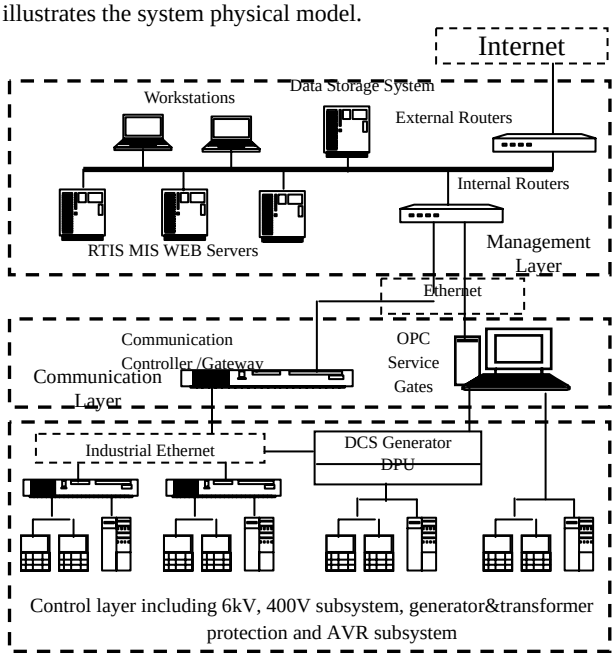


Fig.1. System physical model

1) Control layer includes main protection devices, automatic devices, 400V low voltage systems, 6KV auxiliary power protection and so on. Main protection devices include generator protection, main transformer protection and start-up&stand-by transformer protection. Automatic devices consists of automatic regulator voltage (AVR), automatic transfer switch (ATS) and automatic synchronization systems (ASS) and so on. 400V low voltage systems usually include automatic change-over device, intelligent motor protector, automatic breaker and so on. And 6KV auxiliary power protection includes feeder protection devices, auxiliary transformer integrative protection devices, high-voltage motor integrative protection devices and so on. Furthermore, DCS and FCS are widely used in power plants. And they can make basic operation and control functions. Though DCS including data process unit (DPU), electrical workstation and so on is the most important system in power plants. For hard cable and limited information, it is impossible to complete some complex operations for DCS. FCS has been paid more and more attention, whose communication rate, communication distance and operation capability has greatly exceeded that of DCS [5][6].
2) Communication layer includes communication interfaces, communication devices and so on. In the distributed monitoring system, all kinds of devices and subsystems have their communication models. According to the description above, there are four kinds of subsystems as follow: 400V subsystem, 6KV subsystem, generator&transformer protection subsystem and AVR subsystem. In the system, they can be directly connected into superior system by communication controllers and IPC devices. Or they can be integrated into FCS and DCS that are connected to superior systems by serial ports and industrial Ethernets. For electrical interlock and reliability, hared cables are usually used for communication between DCS and field devices. Generally, FCS and DCS can provide several serial ports such as RS232 to communicate with the distributed monitoring system. And parts of them in electrical systems have utilized TCP protocol for communication in Ethernet model.
3) In our systems, a novel communication device is defined as OPC (OLE Process Control) services gates. OPC services gate consists of micro-processors, buffer and communication ports including serial ports and Ethernet ports. According to the requirements of field devices, it classifies electrical monitoring information, provides direct communication interfaces between superior systems and subsystems, and collects real-time data for electrical field decision-making. And the implement and the key technology of it are introduced in section 3.
4) Management layer consists of the servers for real-time information system (RTS), management information system (MIS), and Web service. Data storage systems of intranets can provide information to servers and clients. Also the layer owns some specific workstation including power plant safety workstation, statistic workstation and so on, which can be industrial PCs, PDA and common workstations. Management layer mainly provides decision information, statistic data and real-time data for power plant managers. Furthermore, it can connect power plants to Internet. Managers can remotely and on-line view all kinds of information through Internet, which can help them make exact and scientific decisions.

2.2 System Logical Model

Similar to system logical model, the system logical model of the distributed monitoring system for power plants is defined as a three-layer structure including data integration layer, operation&transmission layer and presentation layer. Different to system logical model, these layers are distinguished by their respective logical characters. System logical model is illustrated as figure 2. System logical model and some key technologies are discussed as follows.

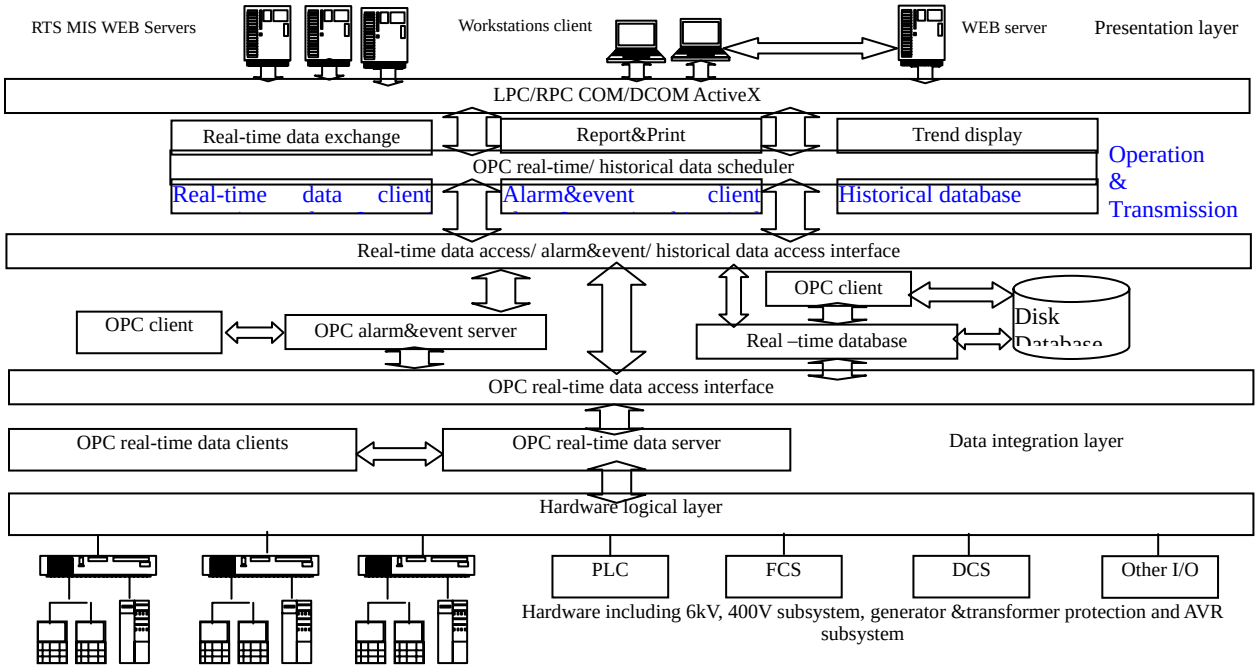


Fig .2. System logical model

1) Data integration layer consists of real-time monitoring subsystem, information data collection subsystem and data access interface. Since there are different monitored signals and all kinds of power electronic devices in power plants, data integration layer can integrate the data coming from different field equipments and provide uniform format interface to distributed monitoring systems.

2) Real-time monitoring subsystem can monitor the field signals including voltage, current, pressure and heat coming from different field ends and equipments. Real-time monitoring subsystem consists of several kinds of hard wares and software, which include IPC, PLC (field control), AD (analog signal data acquisition), DA (analog signal output) and communication&control software corresponding to them. Real-time monitoring subsystem displays real-time state, real-curve, fault-signals and real-time trend figure to distributed monitoring systems. Furthermore, alert examination, on-line fault diagnosis operations and calculations are executed in the subsystem. Then information data collected by the subsystem is transmitted to superior layer and data collection subsystem by data access interface.

3) Data collection subsystem is based on real-time database technology. Different to common disk database, real-time database mainly operates in system memory. And it achieves high real-time by several kinds of buffer and real-time scheduling algorithms classified by data with different real-time requirements. Furthermore some configuration information and frequent-access data are storaged in data collection subsystem. Instead of downloading from superior system, electronic field ends and equipments can directly achieve these information from data collection subsystem.

4) Data access interface consists of communication devices and equipments including RS232/422/485, Ethernet. Also TCP/IP communication protocol for Ethernet and MODBUS protocol for serial port communication are included for communication software. It is difficult to connect all kinds of electronic field devices employing different communication modes for an integrated system. In our system, OPC service gates are employed to solve the problem. And it is discussed in section3.

5) Operation&transmission layer employs data coming from data integration layer to severe for the distributed monitoring system. Generally, the layer consists of a series of function units. Main function units include real-time data transmission, alert&event monitoring, report display, data scheduling and some configuration tools. Different to data integration layer, operation&transmission layer deals with both real-time and unreal-time information. And unreal-time information such as historical power records, historical current curves and client configuration data can be storage in disk databases. In the layer, real-time data coming from data integration layer is classified to transmit for superior layer and to storage in historical database. By historical databases, many reports such as monthly power quantity, fault alert records and so on can be displayed and printed for power plant managers. What is more, electronic engineers and managers can set configuration data for field ends and devices by configuration tools. Also, OPC technology is utilized to simplify system structure, encapsulate logical function units, provide data access interface and so on.

6) Presentation layer consists of RTIS, MIS and Web service systems proposed above. In the layer, clients including engineers and managers can access real-time information, query for specific data and make decisions by GUI (Graphic User Interface). Since power plant information is storaged in operation&transmission layer and data access interfaces have been provided, different applications such as Win32 applications, Web services and C/S databases can conveniently be realized, which communicate with the operation&transmission layer through LPC (Local Process Call), RPC (Remote Process Call) and Socket. Also HTML, Script, ActiveX and COM technologies are utilized in the layer with the recent development of the Internet/Intrant/Infrant. In B/S (Browse/Server) mode, Web servers offers the information services to clients with the processed data in the form of Web pages by accessing databases. And clients can view the information of power plants with a Web browser instead of many complicated applications. For example, an electric power engineer requesting the rotate speeds of some motors opens the homepage for the subject by Internet Explorer and inputs the requests to send to Web servers. Then Web servers for motors can query from real-time databases and offer results to the engineer.

3. OPC SERVICE GATE

In order to connect different subsystems, OPC service gates are employed in the distributed monitoring system. In the section, OPC technology is introduced and the implement and the application of OPC service gate are researched.

(1) OPC Technology

OPC is a kind of technology criterion to solve the communication problem between field management and process control management [7][8]. And it offers a type of standardized communication mechanism for process control management ends to achieve field data. What is more, OPC technology prevents software from depending on specific hardware, which simplifies the development process of control systems.

Based on COM/DCOM technology, OPC adopts client/server mode for its architecture. And it defines field data acquisition ends as OPC servers and regards other ends accessing the data as clients. Furthermore, OPC encapsulates the communication criterions of specific hardware and offers uniform OPC interface for clients. Then the kernel of OPC technology is real-time data access interface (RDAI) and it distinguishes hypersensitive real-time data from common real-time data. OPC formulates a series of criterions such as the Alarm&Event Interface for hypersensitive real-time data, the Historical Data Interface for trend display, history analysis and report, OPC Security criterion, OPC batch criterion, OPC Data Exchange criterion and so on. And Fig 3 shows the architecture of OPC interfaces.

(2) Service Gate

According to as above, OPC service gates are researched and applied in the distributed monitoring system for power plants. Hypersensitive data such as fault information, transnormal voltage signals and so on is distinguished and transmitted to superior layers by OPC service gates. For example, an electrical machine with a deviant rotate speed will be transpired through field sensors and AD by OPC service gates. Then OPC service

gates alarm RTIS and storage alarm&event information to real-time databases.

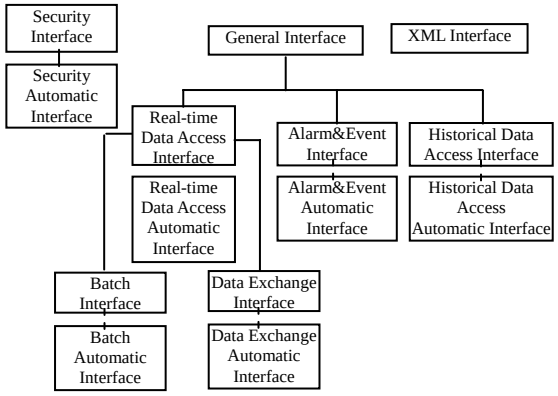


Fig.3. The architecture of OPC interfaces

For the transparent position and plug and play properties of OPC, the number of OPC servers providing information for the system is flexible. When a new device enters into the system, OPC service gates enroll it into the object table and automatically configure the communication parameters of the new object. Then the new device can be certificated by the system and it can communicate with others through OPC service gates. In the system, the structure of OPC service gates consists of server object, group object, item object, data storage area including Card ID, Equipment ID, Value, quality and so on, and communication interface and the structure is illustrated in Fig 4.

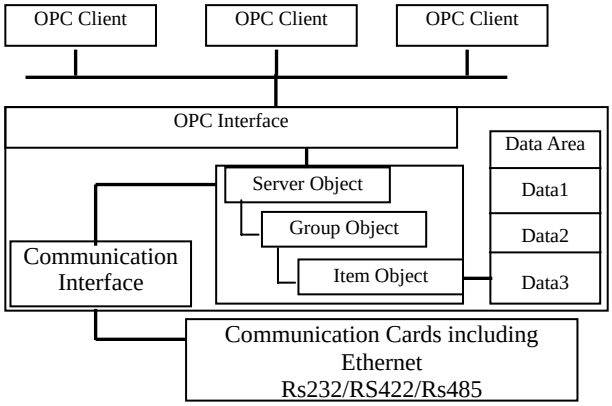


Fig.4. The structure of OPC service gate

4. KEY TECHNOLOGIES

Except for OPC technology, the distributed monitoring system for power plants also employs other technologies to solve problems including reliability, real-time and so on.

(1) Real-Time

In power plants, field signals must be transmitted to superior layers and processed in limited periods. In Ethernet networks, CSMA/CD communication mode is adopted for communication mutual exclusion. Based on the communication mode, TCP/IP is ever prevented from industrial communication for its long delay and randomicity. In the system, system model based on OPC technology utilizes two methods to solve the problems. One method is virtual token technology, and another is multi-thread technology.

In OPC service gates, many server objects is registered in a server table. In order to limit the response delay in a specific period, the number of registered objects must be restricted to guarantee the light load of Ethernet networks. Furthermore, a virtual token is employed to permit server objects to communicate through communication channels. In each OPC service gate, a virtual token scheduler is located, which is responsible for sending tokens to registered objects in limited delay. When an object receives a virtual token, it employs exclusive channels to communicate with others. Also multi-thread technology is employed to ensure system real-time. OPC service gates endow each server object with two threads including monitoring thread and receive/send thread. Monitoring thread is responsible for waiting for information requests coming from others. When a request is received, the monitoring thread will transmit it to the receive/send threads and wait for the next request. Then the receive/send threads insert information data received into the data buffer
area. Fig.5 illustrates the real-time communication model with the two methods.

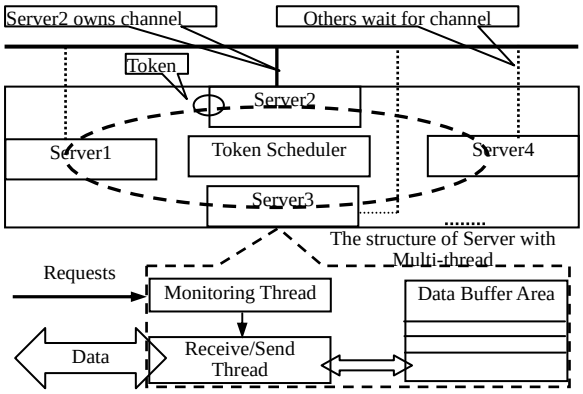


Fig.5. Virtual token and multi-thread

(2) Reliability

In the system, Socket programming is employed for TCP/IP communication. Socket is classified as two kinds including SOCK_STREAM and SOCK_DGRAM. And the first is link-based with TCP protocol and the second is nonlink-based with UDP protocol. TCP protocol communication is based on virtual channel and it can prevent data transmission from disorder, repetition and loss. What is more, TCP protocol asks both communication sides to cooperate with each other to make a link, which guarantee the link to be reliable. Furthermore, TCP protocol utilizes slide window mechanism to ensure transmission efficiency and to prevent networks from congestion. For these advantages, we employ TCP protocol to connect distributed server objects in the system. For example, a device such DCS data processor unit is registered in an OPC service gate with a TCP link. When the device breaks down, the link is destroyed and the OPC service gate can detect the fault and give an alarm. It is link-based communication with TCP that improves the reliability of distributed monitoring systems.

(3) Others

In distributed systems, all monitoring nodes have been endowed with uniform IP addresses. Though many devices are nonEthernet-based, net address transform (NAT) technology is widely utilized to translate specific addresses into IP addresses through address transform tables in OPC service gates. Furthermore, long data packages are usually divided into short data frames and transmitted in communication networks. In order to guarantee the correctness of data, cyclic redundancy check (CRC) method is employed to check received data

The quality of services (QOS) is realized to ensure real-time and reliability of the system. Each message in the system is endowed with a priority according to its real-time and requirements. OPC service gates classify the messages and transmit them referring to their priorities, which guarantee that hypersensitive real-time data can be transmitted in time. For example, OPC service gates receive the configuration information of FCS and the alarm&event message of a DPU. Usually, alarm&event messages have high priorities. Then OPC service gates reprieve the configuration and transmit the alarm&event message immediately.

5. CONCLUSIONS

Distributed monitoring systems for power plants integrate power electronic technology and 3C technology (Computer, Communication and Control technology). And they can provide real-time, reliable and exact to field engineers and managers. The system presented above is realized with many advanced technologies such as OPC technology, token technology and so on. Furthermore, it has been working well, and plays an important role in power plants.

REFERENCES

[1] Anderson T C, *Browser-based performance monitoring integrate thermal, financial information [J]*, Power, 2001,145(5): 79-84.

[2] Jiang H, Xu ZG, Cao ZP, et al. *Designing and implement of data channels in RTMIS for power plant [J]. Automation of Electric Power Systems*, 2002, 26(2): 62-64. (in Chinese)

[3] Xu ZG, Gao ZP, Si FQ, "Real-time information system of power plant based on B/S computing mode [J]", *Journal of Southeast University (English Edition)*, 2002, 18(1): 80-83.

[4] Jin Tao, Tang Tao, Que LY, "Analysis and discussion on decentralized substation automation system [J]". *Automation of Electric Power Systems*, 1997, 21(10): 69-72. (in Chinese).

[5] Dai XH, Wei Wei, Wang Wu, "Implementation of monitoring system of thermal generator based on Profibus in power plant [J]", *Automation of Electric Power Systems*, 2000, 24(16): 51-53. (in Chinese).

[6] Yang Ping, Wu Jie, "Real-time state supervisory system and fault diagnosis for thermal power plant [J]". *Automation of Electric Power Systems*, 2000, 24(17): 37-40. (in Chinese).

[7] Burke TJ, "OPC Vision 2001[EB/OL]", Http://www.opcfoundation.org, 2001,9.

[8] Microsoft. "Microsoft's Vision and Strategies for Manufacturing[EB/OL]".Http://www.microsoft.com, 2002, 2.

Graded Reasoning about Knowledge *

Jun Li
School of Science, Lanzhou University of Technology
Lanzhou,730050,China
Email: lijun@stu.snnu.edu.cn; lijun@lut.cn

ABSTRACT

In many of the application areas for reasoning about knowledge, it is important to reason about the possibility of certain events as well as the knowledge of agents. This paper presents a graded method for reasoning about knowledge which allows us to say that, to what extent an agent knows an event at a given point (M,s) .And some properties about this type of graded methods are discussed.

Keywords: Reasoning About Knowledge, Kripke Structure, Graded Reasoning.

1. INTRODUCTION

Reasoning about knowledge has become an active topic of investigation for researchers in such diverse fields as philosophy[1],economics[2] and artificial intelligence[3] in finding natural semantics for logics of knowledge and belief. Recently the interest of theoretical computer scientists has been sparked, since reasoning about knowledge has been shown to be an useful tool in analyzing distributed systems (see [4-13]for an overview and references).The standard approach to modeling knowledge, which goes back to Hintikka[1],is in terms of possible worlds. The intuitive idea is that besides the true state of affairs, there are a number of other possible states of affairs, or possible worlds. Some of these possible worlds may be indistinguishable from the true worlds to an agent. An agent is then said to know or believe a fact φ if φ is true in all the worlds he consider possible. In many of the application areas for reasoning about knowledge, it is important to reason about the possibility of certain events as well as the knowledge of agents. Fagin and Halpern provide a model for reasoning about knowledge and probability together[14],the language of the model is powerful enough to allow reasoning about high-order probability. Moreover Halpern studies the probabilistic algorithmic knowledge which characterizes the information provided by a randomized knowledge algorithm when its answers have some probability of being incorrect[15].

Recently, different methods for graded reasoning in propositional logics have been proposed and studied (see[16-21] and their references), in this paper, we are going to merge some ideas provided in ref.[17] by Wang into reasoning about knowledge so as to obtain a graded mechanism for reasoning about knowledge.

The rest of this paper is organized as follows. In section 2, we review Kripke structure and the axiom system $\mathbf{S5_n}$.In section 3, we give a graded method for reasoning about knowledge and some of its properties are discussed. We conclude in section 4.

* Supported by the National Natural Science Foundation of China under Grant No.10331010 and the Outstanding Youth Foundation of Lanzhou University of Technology.

2. THE STANDARD KRIPKE MODEL FOR KNOWLEDGE

In this section we briefly review the standard $\mathbf{S5_n}$ possible-worlds semantics for knowledge. The reader is referred to Halpern and Moses[1992] for more details.

In order to reason formally about knowledge, we need a language. Suppose we consider a system consisting of n agents, creatively named $1,2,\cdots,n$ .For simplicity, we assume these agents wish to reason about a world that can be described in terms of a nonempty set Φ of primitive propositions, typically labeled $p_1, p_2, \cdots$ .These primitive propositions stand for basic facts about the world.(For distributed systems application, these will typically represent statements, such as "The value of x is 0";in natural language situations, they might represent statements of the form "It is raining in London.") We construct more complicated formulas by closing off Φ under the Boolean connectives $\neg$, $\wedge$, and the modal operators K_i, for $i=1,2,\cdots,n$ (where $K_i\varphi$ is read "agent i knows φ"). Let $L_n(\Phi)$ be the set of formulas that can be built up starting from the primitive propositions in Φ, using conjunction, negation, and the modal operators. For convenience, we define true to be an abbreviation for the formula $p \vee \neg p$, where p is a fixed primitive proposition. We abbreviate $\neg$***true*** by ***false*.**

We give semantics to these formulas by means of ***Kripke structures***[Kripke,1963],which formalize the intuition behind possible worlds.

Definition 2.1[5] ***A Kripke structure*** M ***for knowledge(for n agents)*** is a tuple $(S,\pi,\Re_1,\cdots,\Re_n)$,where S is a set of states, $\pi(s)$ is a truth assignment to the primitive propositions of Φ for each state $s \in S$ (i.e., $\pi(s)(p) \in \{$***true, false***$\}$ for each primitive proposition $p \in \Phi$ and state $s \in S$),and $\Re_i$ is an binary relation on S ,for $i=1,2,\cdots,n$ .The $\Re_i$ relation is intended to capture the possibility relation according to i : $(s,t) \in \Re_i$ if in world s agent i considers world t possible.

We now define what it means for a formula to be true at a given state in a structure. We define the notion $(M,s) \models \varphi$,which can be read "φ is true at (M,s)" or "φ holds at (M,s)". The $\models$ relation can be defined by induction on the structure of φ as follows:

(i) $(M,s) \models p$ iff $\pi(s)(p) =$ ***true.***($p \in \Phi$).
(ii) $(M,s) \models \neg\varphi$ iff $(M,s) \not\models \varphi$.
(iii) $(M,s) \models \varphi \wedge \psi$ iff $(M,s) \models \varphi$ and $(M,s) \models \psi$.
(iv) $(M,s) \models K_i\varphi$ iff $(M,t) \models \varphi$ for each t such that $(s,t) \in \Re_i$.

The last clause in the above definition captures the intuition that agent i knows φ in world (M,s) exactly if φ is true in all states that agent i considers possible. Let $\mathrm{M}_n^{rst}(\Phi)$ (M_n^{rst} for short) be the class of all Kripke structures for n agents over Φ where the possibility relations are all the equivalent relations.

Definition 2.2[5] Given a structure $M=(S,\pi,\Re_1,\cdots,\Re_n)$,

we say that a formula φ is ***valid*** in M ,and *write* $M\models\varphi$,if $(M,s)\models\varphi$ for every state s in S ,and say that φ is ***satisfiable*** in M if $(M,s)\models\varphi$ for some s in S .We say that a formula φ is ***valid*** ,and write $\models\varphi$, if it is valid in all structures, and it is ***satisfiable*** if it is satisfiable in some structure.

We are often interested in characterizing by an axiom system the set of formulas that are valid. An axiom system AX is said to be sound for a language $\boldsymbol{L}$ with respect to a class $\mathbb{M}$ of structures if every formula in $\boldsymbol{L}$ provable in AX is valid with respect to every structure in $\mathbb{M}$. The system AX is complete for $\boldsymbol{L}$ with respect to $\mathbb{M}$ if every formula in $\boldsymbol{L}$ that is valid with respect to every structure in $\mathbb{M}$ is provable in AX. We think of AX as characterizing the class $\mathbb{M}$ if it provides a sound and complete axiomatization of that class.It is well known that the axiom system $\mathbf{S5_n}$ consists of the following set of axioms and inference rules:

K1. All instances of propositional tautologies

K2. $(K_i\varphi\wedge K_i(\varphi\Rightarrow\psi))\Rightarrow K_i\psi$.

K3. $K_i\varphi\Rightarrow\varphi$.

K4. $K_i\varphi\Rightarrow K_iK_i\varphi$.

K5. $\neg K_i\varphi\Rightarrow K_i\neg K_i\varphi$.

R1. From φ and $\varphi\Rightarrow\psi$ infer ψ .

R2. From φ infer $K_i\varphi$.

Where $i=1,\cdots,n$.

Theorem 2.3[5] $\mathbf{S5_n}$ is a sound and complete axiomatization with respect to M_n^{rst} .

We remark that this axiom system for the case of one agent has traditionally been called **S5**, which has been proved particularly useful in distributed systems application.

3. METHOD OF THE GRADED REASONING ABOUT KNOWLEDGE

In this section, we will introduce the idea of grading knowledge and executing approximate reasoning by using the graded knowledge.We will capture the graded knowledge by introducing the definition of the extent that agent i knows φ at (M,s) . According to the definition of the semantic of $K_i\varphi$ in section 2, we have that

$$(M,s)\models K_i\varphi \text{ iff } (M,t)\models\varphi \tag{3.1}$$

for each t such that $(s,t)\in\Re_i$.

That is to say, agent i knows φ at (M,s) if φ is true at all the worlds that agent i considers possible in world s .In another word, φ is a knowledge of agent i at the state s in the structure M if φ is true at all the worlds that agent i considers possible in world s . We will introduce the notion of "the extent that agent i knows φ" to capture to what extent agent i knows φ .Define

$$\Re_i(s)=\{t\mid(s,t)\in\Re_i\} \tag{3.2}$$

$$T_i^s(\varphi)=\{t\in\Re_i(s)\mid(M,t)\models\varphi\} \tag{3.3}$$

Remark 3.1 Because in most practical application areas, there are only finite many states that agent i considers possible at any given state $s\in S$,hence, we only consider, in the following, the case that $\Re_i(s)$ is a nonempty and finite set for every $s\in S$,i.e.

$$0<|\Re_i(s)|<+\infty \tag{3.4}$$

Where $|\Re_i(s)|$ is the cardinality of $\Re_i(s)$.

Definition 3.2 Suppose that $\varphi\in L_n(\Phi)$, Let

$$\omega_{i,s}(\varphi)=|T_i^s(\varphi)|\ /\ |\Re_i(s)| \tag{3.5}$$

$\omega_{i,s}(\varphi)$ is called the belief degree of agent i w.r.t. φ at state s .

Proposition 3.3 Suppose that $\varphi\in L_n(\Phi)$ then

(i) $\omega_{i,s}(\varphi)=1$ if and only if $(M,s)\models K_i\varphi$,

(ii) $\omega_{i,s}(\varphi)=0$ if and only if $(M,s)\models K_i\neg\varphi$.

Proof. (i) Assume that $(M,s)\models K_i\varphi$, i.e. $(M,t)\models\varphi$ holds for each t such that $(s,t)\in\Re_i$,thus $T_i^s(\varphi)=\Re_i(s)$,it follows from (3.5) that $\omega_{i,s}(\varphi)=1$ .Conversely, assume that $\omega_{i,s}(\varphi)=1$, by (3.5) we have that $|T_i^s(\varphi)|=|\Re_i(s)|$,therefore $T_i^s(\varphi)=\Re_i(s)$,hence it follows from (3.2),(3.3) and (3.1) that $(M,s)\models K_i\varphi$.

(ii) $(M,s)\models K_i\neg\varphi$ iff $(M,t)\models\neg\varphi$ holds for each t such that $(s,t)\in\Re_i$ iff $(M,t)\not\models\varphi$ for each t such that $(s,t)\in\Re_i$ iff $T_i^s(\varphi)=\{\phi\}$ iff $|T_i^s(\varphi)|=0$ iff $\omega_{i,s}(\varphi)=0$.

Proposition 3.4 Suppose that $\varphi\in L_n(\Phi)$, then

$$\omega_{i,s}(\neg\varphi)=1-\omega_{i,s}(\varphi).$$

Proof. Since $(M,s)\models\neg\varphi$ iff $(M,s)\not\models\varphi$, so it is easy to verify that

$$T_i^s(\varphi)\cup T_i^s(\neg\varphi)=\Re_i(s)$$

and

$$T_i^s(\varphi)\cap T_i^s(\neg\varphi)=\phi.$$

Hence we have that

$$|\Re_i(s)|=|T_i^s(\varphi)\cup T_i^s(\neg\varphi)|$$
$$=|T_i^s(\varphi)|+|T_i^s(\neg\varphi)| \tag{3.6}$$

It follows from (3.5) and (3.6) that

$$\omega_{i,s}(\neg\varphi)=1-\omega_{i,s}(\varphi).$$

Proposition 3.5 Suppose that $\varphi,\psi \in L_n(\Phi)$, then

$$\omega_{i,s}(\varphi \wedge \psi) + \omega_{i,s}(\varphi \wedge \neg\psi) = \omega_{i,s}(\varphi).$$

Proof. Firstly, it is no hard to prove the following facts by using $(*)$(iii) and $(*)$(ii) respectively:

$$T_i^s(\varphi \wedge \neg\psi) = T_i^s(\varphi) \cap T_i^s(\neg\psi) \quad \text{and}$$

$$T_i^s(\varphi \wedge \psi) = T_i^s(\varphi) \cap T_i^s(\psi),$$

$T_i^s(\psi) \cup T_i^s(\neg\psi) = \Re_i(s)$ and $T_i^s(\psi) \cap T_i^s(\neg\psi) = \phi$.

Hence we have that

$$\begin{aligned} &T_i^s(\varphi \wedge \neg\psi) \cup T_i^s(\varphi \wedge \psi) \\ &= (T_i^s(\varphi) \cap T_i^s(\neg\psi)) \cup (T_i^s(\varphi) \cap T_i^s(\psi)) \\ &= T_i^s(\varphi) \cap (T_i^s(\neg\psi) \cup T_i^s(\psi)) = T_i^s(\varphi) \cap \Re_i(s) \\ &= T_i^s(\varphi), \end{aligned} \tag{3.7}$$

$$\begin{aligned} &T_i^s(\varphi \wedge \neg\psi) \cap T_i^s(\varphi \wedge \psi) \\ &= (T_i^s(\varphi) \cap T_i^s(\neg\psi)) \cap (T_i^s(\varphi) \cap T_i^s(\psi)) \\ &= T_i^s(\varphi) \cap (T_i^s(\neg\psi) \cap T_i^s(\psi)) \\ &= \phi. \end{aligned} \tag{3.8}$$

As can be seen from (3.7) and (3.8) that

$$\begin{aligned} &|T_i^s(\varphi \wedge \neg\psi)| + |T_i^s(\varphi \wedge \psi)| \\ &= |T_i^s(\varphi \wedge \neg\psi) \cup T_i^s(\varphi \wedge \psi)| - \\ &\quad |T_i^s(\varphi \wedge \neg\psi) \cap T_i^s(\varphi \wedge \psi)| = |T_i^s(\varphi)| \end{aligned} \tag{3.9}$$

Hence it follows from (3.9) and definition 3.2 that

$$\omega_{i,s}(\varphi \wedge \psi) + \omega_{i,s}(\varphi \wedge \neg\psi) = \omega_{i,s}(\varphi).$$

Proposition 3.6 Suppose that $\varphi,\psi \in L_n(\Phi)$, then

$$\omega_{i,s}(\varphi \wedge \psi) + \omega_{i,s}(\varphi \vee \psi) = \omega_{i,s}(\varphi) + \omega_{i,s}(\psi).$$

Proof. Since

$(M,t) \models \varphi \wedge \psi$ iff $(M,t) \models \varphi$ and $(M,t) \models \psi$,

$(M,t) \models \varphi \vee \psi$ iff $(M,s) \models \varphi$ or $(M,t) \models \psi$,

hence it is easy to see that

$$T_i^s(\varphi \wedge \psi) = T_i^s(\varphi) \cap T_i^s(\psi)$$

and

$$T_i^s(\varphi \vee \psi) = T_i^s(\varphi) \cup T_i^s(\psi),$$

and therefore

$$\begin{aligned} &|T_i^s(\varphi \vee \psi)| = |T_i^s(\varphi) \cup T_i^s(\psi)| \\ &= |T_i^s(\varphi)| + |T_i^s(\psi)| - |T_i^s(\varphi) \cap T_i^s(\psi)| \\ &= |T_i^s(\varphi)| + |T_i^s(\psi)| - |T_i^s(\varphi \wedge \psi)| \end{aligned} \tag{3.10}$$

It follows from (3.10) and definition 3.2 that

$$\omega_{i,s}(\varphi \wedge \psi) + \omega_{i,s}(\varphi \vee \psi) = \omega_{i,s}(\varphi) + \omega_{i,s}(\psi).$$

Proposition 3.7 Suppose that $\varphi,\psi \in L_n(\Phi)$, if $\omega_{i,s}(\varphi) \geq \alpha$, $\omega_{i,s}(\varphi \to \psi) \geq \beta$, then

$$\omega_{i,s}(\psi) \geq \alpha + \beta - 1.$$

Proof. Assume that $\omega_{i,s}(\varphi) \geq \alpha$, $\omega_{i,s}(\varphi \to \psi) \geq \beta$, then it follows that

$$|T_i^s(\varphi)| \geq \alpha\,|\Re_i(s)|, \quad |T_i^s(\varphi \to \psi)| \geq \beta\,|\Re_i(s)|.$$

Let $G = T_i^s(\varphi) \cap T_i^s(\varphi \to \psi)$, then $G \subseteq T_i^s(\psi)$. In fact, if $t \in G$, then both $(M,t) \models \varphi$ and $(M,t) \models \varphi \to \psi$ hold, hence $(M,t) \models \psi$ holds and therefore $t \in T_i^s(\psi)$. Since

$$\begin{aligned} |\Re_i(s)| &\geq |T_i^s(\varphi) \cup T_i^s(\varphi \to \psi)| \\ &= |T_i^s(\varphi)| + |T_i^s(\varphi \to \psi)| - |G|, \end{aligned}$$

hence we have that

$$\begin{aligned} |T_i^s(\psi)| &\geq |G| \\ &\geq |T_i^s(\varphi)| + |T_i^s(\varphi \to \psi)| - |\Re_i(s)|. \end{aligned} \tag{3.11}$$

It follows from (3.11) and Definition 3.2 that $\omega_{i,s}(\psi) \geq \alpha + \beta - 1$.

Corollary 3.8 Suppose that $\varphi,\psi \in L_n(\Phi)$, if $\omega_{i,s}(\varphi) = 1$, $\omega_{i,s}(\varphi \to \psi) = 1$, then $\omega_{i,s}(\psi) = 1$.

Definition 3.9 Let φ be a formula in $L_n(\Phi)$, t be a state in S. We call φ a knowledge-generalized formula with respect to t for agent i if $(M,t) \models K_i\varphi$ holds whenever $(M,t) \models \varphi$ holds.

Definition 3.10 Let φ be a formula in $L_n(\Phi)$, s be a given state in S, s is said to be a knowledge-generalized state with respect to φ for agent i if φ is a knowledge-generalized formula with respect to each state t in $\Re_i(s)$ for agent i.

Proposition 3.11 Suppose that $\varphi \in L_n(\Phi)$, then

$$\omega_{i,s}(K_i\varphi) \leq \omega_{i,s}(\varphi).$$

Proof. It only needs to prove that $T_i^s(K_i\varphi) \subseteq T_i^s(\varphi)$. In fact, if $t \in T_i^s(K_i\varphi)$, i.e. $t \in \Re_i(s)$ and $(M,t) \models K_i\varphi$, since $\Re_i$ is an equivalent relation and hence $\Re_i$ is reflexive, so $(t,t) \in \Re_i$, then it follows that $(M,t) \models \varphi$, i.e. $t \in T_i^s(\varphi)$, as desired.

Proposition 3.12 Suppose that $\varphi \in L_n(\Phi)$, if the state s is a knowledge-generalized state with respect to φ for agent i, then

$$\omega_{i,s}(K_i\varphi) = \omega_{i,s}(\varphi).$$

Proof. By proposition 3.11, we only need to prove that $\omega_{i,s}(\varphi) \leq \omega_{i,s}(K_i\varphi)$, and it suffices to prove that $T_i^s(\varphi) \subseteq T_i^s(K_i\varphi)$. If $t \in T_i^s(\varphi)$, then $t \in \Re_i(s)$ and $(M,t) \models \varphi$. Since s is a knowledge-generalized state with respect to φ for agent i, hence it follows from Definition 3.10 and definition 3.9 that $(M,t) \models K_i\varphi$ holds for each $t \in \Re_i(s)$, thus $t \in T_i^s(K_i\varphi)$, as desired.

Suppose that $\Gamma \subseteq L_n(\Phi)$, we denote by $D(\Gamma)$ the set of all Γ – conclusions in the following.

Proposition 3.13 Suppose that $\Gamma \subseteq L_n(\Phi)$, and $\omega_{i,s}(\varphi) \geq \alpha$ holds for every $\varphi \in \Gamma$ and ψ is a Γ – conclusion of length n, if the state s is a knowledge-generalized state with respect to each $\varphi \in D(\Gamma)$ for agent i, then

$$\omega_{i,s}(\psi) \geq u_n(\alpha - 1) + 1, \tag{3.12}$$

where μ_n is the n-th term of the Fibonacci sequence, i.e.

$$u_n = \frac{1}{\sqrt{5}}\left[\frac{1+\sqrt{5}}{2}\right]^n - \frac{1}{\sqrt{5}}\left[\frac{1-\sqrt{5}}{2}\right]^n \qquad n = 1,2,\cdots .$$

Proof. A Fibonacci sequence is a sequence $u_1, u_2, \cdots$ with $u_1 = u_2 = 1$ and satisfying $u_n + u_{n+1} = u_{n+2}$ $(n = 1,2,\cdots)$ .In case $n = 1$,it follows from the fact that either $\psi \in \Gamma$ or ψ is an axiom that $\omega_{i,s}(\psi) \geq \alpha = u_1(\alpha - 1) + 1$ holds, i.e. (3.12) holds for $n = 1$. Assume that (3.12) holds for every $n \leq k$, ψ is a $\Gamma -$ conclusion of length $n+1$ and the deduction sequence is $\varphi_1, \varphi_2, ..., \varphi_k, \psi$. It only needs to consider the case that $\psi \notin \Gamma$ and ψ is not an axiom and then we need only to consider the following two cases:

(i) There exist φ_j and φ_l $(j, l \leq k)$ such that ψ is deducted from φ_j and φ_l by using rule of Modus Ponens. Say $l < j$ and $\varphi_j = \varphi_l \to \psi$ .It follows from the induction hypothesis that

$$\omega_{i,s}(\varphi_l) \geq u_l(\alpha - 1) + 1 \geq u_{k-1}(\alpha - 1) + 1,$$
$$\omega_{i,s}(\varphi_j) \geq u_j(\alpha - 1) + 1 \geq u_k(\alpha - 1) + 1.$$

Hence we get from Proposition 3.7 that

$$\begin{aligned}\omega_{i,s}(\psi) &\geq \omega_{i,s}(\varphi_l) + \omega_{i,s}(\varphi_j) - 1 \\ &\geq u_{k-1}(\alpha - 1) + u_k(\alpha - 1) + 1 \\ &= u_{k+1}(\alpha - 1) + 1\end{aligned}$$

i.e. (3.12) holds for $n = k + 1$.

(ii) There exist φ_j $(j \leq k)$ such that ψ is obtained from φ_j by using the rule of Knowledge Generalization, i.e. $\psi = K_i\varphi_j$. Since the state s is a knowledge-generalized state with respect to each $\varphi_j \in D(\Gamma)$ for agent i , it follows from Proposition 3.12 and the induction hypothesis that

$$\begin{aligned}\omega_{i,s}(\psi) &= \omega_{i,s}(K_i\varphi_j) = \omega_{i,s}(\varphi_j) \\ &\geq u_k(\alpha - 1) + 1 \geq u_{k+1}(\alpha - 1) + 1\end{aligned}$$

i.e. (3.12) holds for $n = k + 1$ .This completes the proof of Proposition 3.13.

4. CONCLUSIONS

The goal of this paper is to provide a graded method for reasoning about knowledge which allows us to say: to what extent an agent knows an event at a given state s , under a given Kripke structure M .we consider the graded reasoning, in this paper, only at a given state under a given structure. In many practical applications, we need to define the extent that an agent i knows an event φ at a given structure M , or the extent that an agent i knows an event φ ,all these above issues we will discuss in the next paper.

REFERENCES

[1] J.Hintikka, *Knowledge and Belief, Ithaca*: Cornell University Press, 1962.

[2] R.J. Aumann, "Agreeing to disagree", *Ann.Stat*, Vol.6, No.41976, pp.1236-1239.

[3] R.C.Moore, "A formal theory of knowledge and action",In *Formal Theories of the Commence* World,J. Hobbs and R.C.Moore,eds.Ablex PublishingCorp, Norwood, pp319-358

[4] J.Y.Halpern, "Using reasoning about knowledge to analyze distributed systems",in *Annual Review of Computer Science*,Vol.2,37-68. Palo Alto: Annual Reviews Inc., 1987.

[5] R.Fagin,et,al,*Reasoning about Knowledge, London*: The MIT Press,1996.

[6] Y.Shoham, "Agent oriented programming", *Artificial Intelligence*,Vol.60,No.1,1993,pp.51-92.

[7] K.Binmore,H.S.Shin, "Algorithmic knowledge and game theory",in *Knowledge,Belief,and Strategic Interaction*,New York:Cambridge University Press, 1993.

[8] J.Y.Halpern, M.R. Tuttle, "Knowledgr, probability, and Adversaries" ,*Journal of ACM*,Vol.40,No.4, 1993, pp.917-960.

[9] M.Dekhtyar,A.Dikovsky,M.Valiev, "On complexity of verification of interacting agents'behavior", *Artificial Intelligence*,Vol.141,2006,pp.336-362.

[10] E.T. Mueller, "Event calculus and temporal logics compared",*Artificial Intelligence*,Vol.170,2006,pp.1017-1029.

[11] P.Blackburn,M.Rijke,Y.Venema,*Modal Logic,Madrid*: Cambridge University Press,2001.

[12] Liu W. "Analyzing the degree of comflict among belief functions", *Artificial Intelligence*, Vol.170, 2006, pp. 909-924.

[13] G.Lamperti, M.Zenella. "Flexible diagnosis of discrete-event systems by similarity-based reasoning techniques", *Artificial Intelligence*, Vol.170, 2006, pp. 232-297.

[14] R.Fagin, J.Y.Halpern, "Reasong about knowledge and probability",*Journal of the ACM*,Vol.41,No.2,1994, pp.340-367.

[15] J.Y.Halpern, R.Pucella," Probabilistic algorithmic knowledge, Logical Methods" in *Computer Science*, Vol.1 No.3:1, 2005,pp.1-26.

[16] Ying Mingsheng. "A logic for approximate reasoning", *J.Symb.Logic*,Vol.59,1994,pp.830-837.

[17] Wang Guojun,et al, "Theory of truth degrees of propositions" In *two-valued logic. Science of China*(Ser.A),Vol.45,No.9,2002, pp.1106-1116.

[18] Li Jun, et al, "Theory of truth degrees of propositions in Lukasiewicz n-valued propositional logic", *Acta Mathematica* Sinica,Vol.47,No.4,2004, pp.769-780.

[19] Li Jun,Wang Guojun,"Theory of truth degrees of propositions in the logic system Ln^{*v}",*Science in China*(Ser.F)Vol.49,No.4,2006, pp.471-483.

[20] Li Jun,Wang Guojun, "Theory of α-truth degrees in n-valued gödel propositional logic", *Journal of Software*, Vol.18,No.1,2007, pp.33-39.

[21] Wang Guojun, Zhang Wenxiu, "Consistency degrees of finite theories in Lukasiewicz propositional fuzzy logic",*Fuzzy Sets and Systems*, Vol.149, No.2,2005, pp.275-284.

Jun Li is an assistant professor of School of Science , Lanzhou University of Technology. He graduated from Shaanxi Normal University in 2002 and obtained his Master degree. And now, he is a graduate studying in the college of mathematics and information science, Shaanxi Normal University, majored in Uncertainty reasoning, expecting to

receive his Ph.D one year later. He has published over 30 Journal papers. His research interests are in reasoning about knowledge, uncertainty reasoning and non-classical mathematical logic.

A Novel Method for the Identification of Nonlinear Systems*

Shilian Xu[1], Xingliang Zhu[2], Shenglin Li[1]
[1]Department of Logistics Information Engineering,Logistical Engineering University
Chongqing, 400016, China
[2]School of Management, Chongqing Jiaotong University
Chongqing, 400074, China
Email: [1]swaol2008@yahoo.com.cn,[2]z3x3l3@163.com

ABSTRACT

In the identification of the nonlinear subsystem of Hammerstein systems, the estimates obtained from the conventional polynomial least-squares method cannot have a satisfactory result for a small number of data. Especially, the results can be very bad at the boundary of the observation range. In this paper, we use the spline functions modeling the nonlinear subsystem in the Hammerstein system. To identify the spline functions, a constrained least-squares algorithm is proposed. Finally, to demonstrate the effectiveness of the proposed method, simulation results are illustrated.

Keywords: Nonlinear Subsystem, Hammerstein Systems, Identification, Spline Function, Subsystem

1. INTRODUCTION

The key problem in system identification is to find a suitable model structure, within which a good model is to be found. Linear system theory is very well developed and there exist many results that can be applied to the obtained linear model. However, there are no universal models and identification methods for general nonlinear systems. In this paper, we consider the identification problem of nonlinear Hammerstein system. A Hammerstein system is consisted of two subsystems connected in cascade: a nonlinear memoryless subsystem followed by a linear memory subsystem.

As we known, Conventional identification methods for the nonlinear subsystem have many shortcomings [1-3]. To overcome those problems, we propose to model the nonlinear subsystem using spline functions. For simplicity, we only consider the linear and quadratic spline functions. In curve fitting, the spline functions are known to be better than the polynomials. Thus, we expect that they can also well model the nonlinear subsystem in the Hammerstein. A constrained least-squares (CLS) identification algorithm is considered, and Constrains are imposed to ensure the continuity and smoothness of the nonlinear function. Simulations show that the proposed method outperforms the existing algorithms including parametric or nonparametric one.

First, the proposed methods are presented in Section 2. Simulations comparisons for conventional methods are made in Section 3. Finally, the conclusions are drawn in Section 4.

2. THE PROPOSED ALGORITHM

The estimates obtained from the polynomial LS (Least-Squares) method cannot have a satisfactory result for a small number of data [2-6]. Especially, the results can be very bad at the boundary of the observation range. We propose to use the linear and quadratic spline functions modeling the nonlinear subsystem in the Hammerstein system. The nonlinear function is first divided into several sections. The function in each section is modeled by a first or second order polynomial.

The nonlinear function is first divided into K sections and the function in each section is modeled by a first or second order polynomial. Thus, the LS method can be applied to each section. To do that, inputs and outputs are classified into the *K* sections. Let the input vector in the ith group be denoted as X_i and the corresponding output vector as $\hat{Y}_i$. Let

$$X_i = T_i X \tag{1}$$

Where X is the total input vector and T_i is a grouping matrix having the form

$$T_i = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}_{N_i \times N} \tag{2}$$

Where N is the order of X and N_i is the number of observations in the ith section. Then the output vector of the ith section can be represented as [6, 7, 8, 9, 10]

$$\hat{Y}_i = T_i \hat{G}(a_i X_s + b_i X + c_i U) \tag{3}$$

Thus, the normal equation in for the ith section can be presented with $X_{si} = T_i \hat{G}$, $X_i = T_i \hat{G} X$, $U_i = T_i \hat{G} U$, $Y_i = T_i G Y$.

$$\begin{bmatrix} Y_i^T U_i \\ Y_i^T X_i \\ Y_i^T X_{si} \end{bmatrix} = \begin{bmatrix} X_{si}^T U_i & X_i^T U_i & U_i^T U_i \\ X_{si}^T X_i & X_i^T X_i & U_i^T X_i \\ X_{si}^T X_{si} & X_i^T X_{si} & U_i^T X_{si} \end{bmatrix} \begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} + E_i \tag{4}$$

Where a_i; b_i; c_i are the coefficients of the ith section. Let Z_i represent the vector in the left-hand side in Eq. (4), H_i represent the matrix in the right-hand side in Eq. (4), P_i represent the vector in the right-hand side in Eq. (4). We then have

$$Z_i = H_i P_i + E_i \tag{5}$$

The *K* normal equations like Eq. (4) can be combined to form the normal equation of the whole system.

$$\begin{bmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_K \end{bmatrix} = \begin{bmatrix} H_1 & 0 & \cdots & 0 \\ 0 & H_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & H_K \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_K \end{bmatrix} + E \tag{6}$$

Where $E = \begin{bmatrix} E_1 & E_2 & \cdots & E_K \end{bmatrix}^T$. Let Z represent the vector in the left-hand side of Eq. (6), H represent the matrix in the right-hand side in Eq. (6), P represent the vector in the right-hand side of Eq. (6). Then, we have

$$Z = HP + E \tag{7}$$

If the *LS* for each section is carried out individually, they may not be continuous and smooth at the connections. Thus, some constraints must be added. We now show an

* This paper is supported by the Youth Foundation of Logistical Engineering University and the Project of the Chongqing Municipal Education Commission (No. KJ070409)

example where $K = 4$. Let $x_0; x_1; x_2; x_3; x_4$ are points sectioning the nonlinear function. To make the curve continuous, we have to satisfy the following constraints.

$$\begin{cases} c_1 - c_2 = x_1^2(a_2 - a_1) + x_1(b_2 - b_1) \\ c_2 - c_3 = x_2^2(a_3 - a_2) + x_2(b_3 - b_2) \\ c_3 - c_4 = x_3^2(a_4 - a_3) + x_3(b_4 - b_3) \end{cases} \quad (8)$$

To make the curve be smooth, we have satisfied the following constraints.

$$\begin{cases} b_1 - b_2 = -2x_1(a_1 - a_2) \\ b_2 - b_3 = -2x_2(a_2 - a_3) \\ b_3 - b_4 = -2x_3(a_3 - a_4) \end{cases} \quad (9)$$

Substituting Eq. (8) by Eq. (9), we obtain

$$\begin{cases} c_1 - c_2 = x_1^2(a_1 - a_2) \\ c_2 - c_3 = x_2^2(a_2 - a_3) \\ c_3 - c_4 = x_3^2(a_3 - a_4) \end{cases} \quad (10)$$

From Eq. (9) and Eq. (10), P can be represented as

$$\begin{bmatrix} a_1 - a_2 \\ a_2 - a_3 \\ a_3 - a_4 \\ a_4 \\ b_1 - b_2 \\ b_2 - b_3 \\ b_3 - b_4 \\ b_4 \\ c_1 - c_2 \\ c_2 - c_3 \\ c_3 - c_4 \\ c_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ b_1 \\ c_1 \\ a_2 \\ b_2 \\ c_2 \\ a_3 \\ b_3 \\ c_3 \\ a_4 \\ b_4 \\ c_4 \end{bmatrix} \quad (11)$$

Let D represent the vector in the left-hand side of Eq. (11), F represent the matrix in the right-hand side in Eq. (11), P represent the vector in the right-hand side in Eq. (11). Then, $D = FP$, and

$$\begin{bmatrix} a_1 - a_2 \\ a_2 - a_3 \\ a_3 - a_4 \\ a_4 \\ b_1 - b_2 \\ b_2 - b_3 \\ b_3 - b_4 \\ b_4 \\ c_1 - c_2 \\ c_2 - c_3 \\ c_3 - c_4 \\ c_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -2x_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2x_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2x_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 2x_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2x_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2x_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 - a_2 \\ a_2 - a_3 \\ a_3 - a_4 \\ a_4 \\ b_4 \\ c_4 \end{bmatrix} \quad (12)$$

Let M represent the matrix in the right-hand side of Eq. (12), C represent the vector in the right-hand side of Eq. (12). Then, $D = MC$. Eq (6) can be rewritten as

$$Z = HP + E = HF^{-1}MC + E = QC + E \quad (13)$$

Where $Q = HF^{-1}M$. We then obtain a set of linear equations and we can estimate C using the standard LS method.

$$\hat{C} = \left[Q^T Q \right]^{-1} Q^T Z \quad (14)$$

The *CLS* derivation for the linear spline function is similar to that for quadratic one. Here, we only are give the results. Let $X_i = T_i \hat{G} X$, $U_i = T_i \hat{G} U$, $Y_i = T_i G Y$. Then the normal equation for the ith section can be represented as follows.

$$\begin{bmatrix} Y_i^T U_i \\ Y_i^T X_i \end{bmatrix} = \begin{bmatrix} X_i^T U_i & U_i^T U_i \\ X_i^T X_i & U_i^T X_i \end{bmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix} + E_i' \quad (15)$$

Where a_i; b_i are the coefficients of the function in the ith section. Let Z_i' represent the vector in the left-hand side of Eq. (15), H_i' represent the matrix in the right-hand side of Eq. (15), P_i' represent the vector in the right-hand side of Eq. (15), i.e. $Z_i' = H_i' P_i' + E_i'$. The K normal equations like Eq. (15) can be combined to form the normal equation of the whole system.

$$\begin{bmatrix} Z_1' \\ Z_2' \\ \vdots \\ Z_K' \end{bmatrix} = \begin{bmatrix} H_1' & 0 & \cdots & 0 \\ 0 & H_2' & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & H_K' \end{bmatrix} \begin{bmatrix} P_1' \\ P_2' \\ \vdots \\ P_K' \end{bmatrix} + E' \quad (16)$$

Where $E' = \begin{bmatrix} E_1' & E_2' & \cdots & E_K' \end{bmatrix}^T$. Let Z' represent the vector in the left-hand side of Eq. (16), H' represent the matrix in the right-hand side in Eq. (16), P' represent the vector in the right-hand side of Eq. (16). Then

$$Z' = H'P' + E' \quad (17)$$

Adding constraints to ensure the continuity of the estimated nonlinear function, we have D'; F' [similar to D; F in Eq. (11)] and M'; C' [similar to M, C in Eq. (12)]. Then

$$Z' = H'P' + E' = H'(F')^{-1}M'C' + E' = Q'C' + E' \quad (18)$$

Where $Q' = H'(F')^{-1}M'$. Then LS solution for C' is

$$\hat{C}' = \left[(Q')^T \quad Q' \right]^{-1} (Q')^T Z' \quad (19)$$

3. SIMULATION RESULTS

In this section, we carry out simulations to evaluate the performance of the proposed method. The polynomial LS method, the Legendre orthogonal expansion method, and the kernel regression estimate are all compared.

After the parameters of the Hammerstein are all identified, we estimate the system output using the identified parameters for 100 samples. The output signal to noise ration (*SNR*) is used as the performance measure. The output SNR is defined as

$$SNR = \frac{E\left\{ y^2(n) \right\}}{E\left\{ [y(n) - \hat{y}(n)]^2 \right\}} \quad (20)$$

The expectation is approximated using averaging. In our simulations, the results for 50 runs are averaged. The output SNR for different methods versus input observation length is shown in Fig.1. This figure shows that the proposed *CLS* algorithm is superior to others. Though the kernel regression estimate and the *CLS* perform similar when the number of input observation is large, the *CLS* algorithm performs better when the number of input observation is small. The performance of Legendre polynomial expansion is poor.

Since kernel regression and the CLS seemed have the most similar performance, the comparison of output SNR of kernel regression and constrained least square (CLS) versus different input SNR in Fig.2 was made. The input SNR is defined as the ratio of the input x and the noise z in the Hammerstein system.

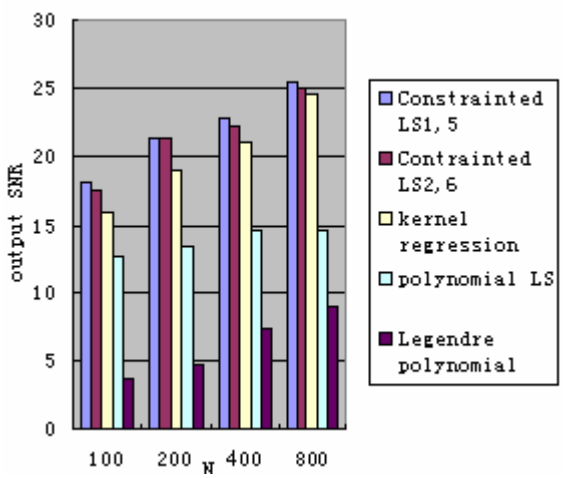


Fig. 1. Comparison of output SNR of different methods versus N=100, 200, 400, 800.

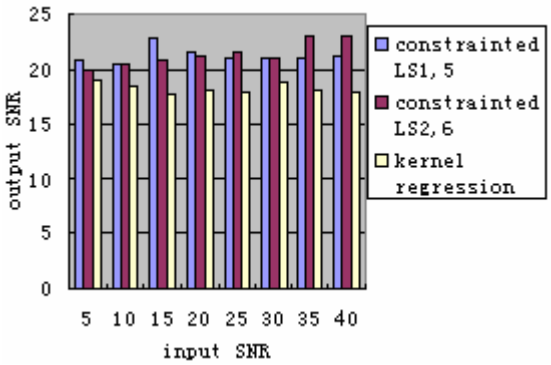


Fig. 2. Comparison of output SNR of kernel regression and LS methods versus input SNR, N=200

4. CONCLUSIONS

In this paper, we consider the identification of Hammestein nonlinear systems. A Hammerstein system is a cascade of a nonlinear memoryless subsystem and a linear subsystem. Conventional parametric identification methods model the nonlinear subsystem using high-order polynomials, which performs poorly for a short training sequence. We used spline functions to solve the problem. To identify the spline functions, we proposed the CLS (Constrained Least-Squares) algorithm. Simulations have demonstrated the effectiveness of our algorithm.

REFERENCES

[1] W. Greblicki and M. Pawlak, "Nonparametric Identification of Hammerstein Systems", *IEEE Trans,Inform,Theory*, vol.IT-35,1989, pp.409-418.

[2] W. Yu and A.S. Poznyak, "System identification with partial-state measurement via dynamic multilayer neural networks", *International Joint Conference, Neural Networks*, vol. 3 ,1999,pp.2081 -2086.

[3] M. Ibukahla,J. Sombria,F. Castanie, N.J. Bershad, "Neural networks for modeling nonlinear memoryless communication channels", *IEEE Transactions, Communications*, vol. 45,no.7,July 1997,pp.768 -771.

[4] W. Greblicki and M. Pawlak, " Nonparametric Identification of Hammerstein Systems,"*IEEE Trans. Inform.Theory*,vol.IT-35,1989,pp.409-418.

[5] M. Pawlak,"On the Series Expansion Approach to the Identification of Hammerstein Systems," *IEEE Trans. Automat.Contr*,vol.36,no.6,1991,pp.763-767.

[6] P. Hall, "Integrated square error properties of Kernel estimators of regression functions,"Ann.Statist,vol.12, 1984,pp.241-260.

[7] S.A.Billings and S.Y.Fakhouri, "Nonlinear system identification using the Hammerstein model,"Int.J. Systems Sci,vol.10,No.5,1979,pp.567-578.

[8] L.X.Li,M.R.F, T.C.Y, "Gaussian-basis-function neural network control system with net-work-induced delays," in *Proc. IEEE Intl. Conf. on Machine Learning and Cybernetics*,vol.3,2002,pp.3-1536.

[9] W.Y.Wang, C.Y.Cheng, Y.G.Leu,"n online GA-Based Output-Feedback Direct Adap-tive Fuzzy-Neural Controller for Uncertain Nonlinear Systems",*IEEE Trans. on Systems,Man and Cybernetics*,vol.34,2004, pp.334-345.

[10] G.Matronardi,V.Bevilacqua,"Video Saurus system: movement evaluation by a genetic algorithm," in *Proc. IEEE Intl. Symm. on Computational Intelligence for Measurement Systems and Applications*,2003,pp.49-51.

The QoS Requirement and Solutions for the Internet-based Fire Remote Monitoring System

Hongwei Zhu, Caijiao Xue, Dongdong Hu
Fire Command Department, Chinese People's Armed Police Force Academy
Langfang, Hebei, China , 065000
Email: zhw_xcj@sina.com

ABSTRACT

With the explosive development of the Internet, it provides a platform for the realization of remote real-time monitoring of large city fires at a low cost. In this article, first the application background of the Internet-based fire remote monitoring system is introduced. Then the characteristics and the QoS requirements (i.e. real time, reliability and security) for the system are analyzed. Finally solutions for each QoS requirement are proposed and discussed.

Keywords: Internet, Real-time System, QoS (Quality of Service),Fire Remote Monitoring System

1. INTRODUCATION

With the popularization and development of the Internet, it almost extends everywhere over the world, and gradually turns into the versatile platform for various interesting and useful applications. At the same time, the Internet offers a good opportunity for the realization of remote monitoring of large city fires at a low cost. However, with the portfolio transmitted through Internet becoming larger and larger, the QoS (Quality of Service) becomes the key problem which decides whether every operation can be transmitted smoothly. The Internet-based fire remote monitoring system is also confronted with the same problem[1].

The basic QoS requirement for the Internet-based fire remote monitoring system is real-time, reliability and security. Aside from this, according to the characteristics of remote monitoring of fires, special QoS requirement might be needed for practical applications, which forms the multidimensional QoS. Solutions for multidimensional QoS parameters are also to be found out. This paper has presented an analysis of the QoS requirements for the Internet-based fire remote monitoring system, and proposed the correspondent solutions, which would be helpful for the design and development of fire remote monitoring system based on Internet.

2. THE APPLICATION BACKGROUND

Currently fire monitoring systems have been fixed in most new buildings throughout China, but most of the monitoring systems is based on LAN, and could only be realized in single buildings. Some fire monitoring systems get in touch with the fire department through special channels. Special channel is very expensive, which causes resource waste.

With the development of Internet and broad band technology, it provides a sound communication channel for the fire remote monitoring system. In other words, the information of the fire remote monitoring system can be transmitted via Internet. The system works in such a manner: establish different types of communication protocols in the network modules (which are embedded in the fire alarm controllers), so that the alarm information can be transferred to the Internet in the TCP/IP format, and thus real-time monitoring of fire alarm controllers through the Internet can be realized. This mode has resolved the mismatch problem of equipment protocols from different manufacturers, and it also has the advantages of low cost, networking convenience, good expandability etc.[2].

3. ANALYZING THE QOS REQUIREMENT

3.1 The Real-time Requirement

The fire remote monitoring system is an automated installation which is mounted in buildings to discover and report a fire in an early stage. It is an indispensable component in modern fire safety engineering. Incipient alarm of fires is the most effective measure to extinguish fires and protect property from damage. The earlier the fire is discovered, the more timely the fire is suppressed. Otherwise a small fire may spawn a dramatic calamity, which is likely to bring about large casualties and damages. The mission of the fire remote monitoring system is to discover the fire in time, so the real-time requirement is of significant importance to the system.

However, data on Internet is stored and transmitted as data packet via virtual connections, which would result in time delay. Router is the core of Internet net structure. It transmits IP packets according to the principle of first come, first served. The reason which causes the delay of IP packets can be concluded as two aspects. One is the searching time of the router; the other is the queue time of IP packets. Especially severe delay will occur when the network is jammed up. What's more, when the queue is full some IP packets would be discarded, which would cause the lost of data during network transmitting. Therefore, the delay of data transmission on Internet must be resolved for the Internet-based fire remote monitoring technology.

Generally speaking, we can define the delay time in the data transmitting process as the QoS index. The fire remote monitoring system requires that the delay time should not exceed a certain upper limit.

3.2 The Reliability Requirement

In the development of Internet, the reliability of service is becoming an increasingly important problem. Owing to the great importance of the fire remote monitoring system, the lost of fire monitoring information can bring about tremendous loss. A general system often requires rather high fault-tolerance. Conventional reliability indexes are defined in terms of statistical indexes such as the lapse rate, the average lapse time, the lapse interval time, the mean time to repair, and the malfunction coverage rate, etc. As for the fire remote monitoring system, generally the reliability measures such as backup numbers, active/passive copy etc, can be used as the QoS indexes.

3.3 The Security Requirement

As the network grows with an explosive speed, the network security has been considered of vital importance by network administrators and users. In fact, many individual networks

have already been forced to retreat from the Internet because their security was menaced. In the same way, whether the fire remote monitoring system can work normally on the Internet isstrongly dependent on the security of the system.

The securities of network application service have several sides. The securities of the Internet-based fire remote monitoring system in terms of the QoS index should include three aspects as following:

(1) Security of the network and the application platform. It mainly includes the reliability and viability of the network, and the reliability and usability of the information system. The reliability and viability of the network is guaranteed by the environment security, physical security, node security, link security, topology security, structure security etc. The reliability and usability of the information system can refer to that of the computer system.

(2) Security of the Application Service. It involves the usability and controllability of the application service. The former is guaranteed by service connection security, service anti-attack ability, surveillance of the application service by the state etc. The latter is correlated with the reliability and the maintenance ability of the network.

(3) Security of information processing and transmission. It consists of the integrality, confidentiality and incontestability of information during transmission and storage. The integrality of information can be ensured by message discrimination mechanism such as Ha-xi algorithm. The confidentiality of information can be guaranteed by encryption mechanism and cryptographic key distribution. The incontestability of information can be safeguarded by the digital signature technique.

4. QOS SOLUTIONS

4.1 Solutions for Real-time Requirement

To settle the real-time problem of the fire remote monitoring system, the emphasis should be laid on the settlement of the time delay problem as the fire information is being transmitted on the Internet. The time delay consists of several parts, i.e. table-checking delay (by routers), packing delay, transmission delay, propagation delay, queuing delay and processing delay. Among them table-checking delay, packing delay and queuing delay are main factors which cause the time delay on networks.

4.1.1 Reduce The Delay Time of Routers

The key problem for the system lies in how to reduce the delay time of routers. Is it possible to endow the routers with artificial intelligence so that the routers could distinguish the type of information and allow the urgent information pass through the router earlier by jumping the queue? To realize the queue-jump transmission of emergency information without affecting the justice of data transmitting, two requirements need to be fitted. First the information is small; second the transmission frequency is low. Two methods can be used to shorten the time delay of routers.

A) Method of identification of the IP packet for emergency information

IPv4 (Internet Protocol version 4) is the 4th version of the Internet Protocol (IP). It is widely applied and running on hundreds of millions of computers currently. The field of service type in IPv4 header has some parameters which are used in certain networks to indicate the required services. Some networks will provide services with different priority levels. The meaning of each bit in the IPv4 header can refers to Table 1. Below the IPv4 protocol is used to implement the identification of the IP packet for emergency information. As the 7th bit in the service-type field of the IPv4 header is left unused, we can use it to represent the emergency state of the information. If the 7th bit equals 1, the IP packet is emergency information; if the 7th bit equals 0, then the IP packet is common information.

1-2	3	4	5	6	7
Priority	delay	throughput	reliability	reservation	reservation

Table 1. The service-type field of the IPv4 header[3]

B) Method of reducing the time delay in routers for the transmission of emergency information

Following, we will take the parallel-processing exchange-type router as an example, to elaborate on how to reduce the time delay in routers for the transmitting of emergency information. Two approaches can be used to achieve this goal. One approach is to accelerate the search speed of routers; the other is to reduce the time delay on queuing for the emergency information during rush hours.

With the development of the Internet, the network addresses grow more and more, the size of the router table becomes larger and larger, and the time expended on router search in the whole router table becomes longer and longer. As the number of destination addresses for emergency information is quite small, a special local router table can be established to search for the destination addresses of emergency information. In this way the time delay would be reduced markedly.

4.1.2 Shorten The TIme Delay of Propagation in Network Medium

As the router could transmit the IP packet of emergency information immediately and the possibility of data missing is decreased, the last factor influencing the time delay is propagation delay. The router table for emergency information can be generated off line based on the shortest routing selection principle. The shortest routing could be found between any two nodes by Floyd algorithm[4], that is, begin from the original distance matrix, then consider in turns every node in the network as middle node, and update the value of distance matrix constantly until convergence. Suppose that there are N nodes in the network, U is the distance matrix, U_{jk} the element of distance matrix (denoting the distance between node j and node k), R the continuous distance matrix, and R_{jk} the element of R distance matrix, then the Floyd algorithm can be implemented in following steps:

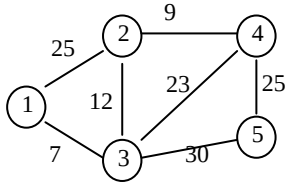


Fig.1. Structure of the network

1) Initialization: For $j = 1,2,\cdots,N$, $k = 1,2,\cdots,N$, set $U_{jk} = d_{jk}$, where d_{jk} is the distance between node j and node k. While they are not directly connected, set the value of d_{jk} as ∞. Set $r_{jk} \to k$, while $j = k$,

$r_{jk} \to 0$. For the network configured like Fig.2, the original distance-matrix is equation (1).

$$U^{(0)} = \begin{bmatrix} 0 & 25 & 7 & \infty & \infty \\ 25 & 0 & 12 & 9 & \infty \\ 7 & 12 & 0 & 23 & 30 \\ \infty & 9 & 23 & 0 & 8 \\ \infty & \infty & 30 & 8 & 0 \end{bmatrix} \quad (1)$$

2) For $i = 1,2,\cdots,N$, go along from the third step to the fifth step;
3) For $j = 1,2,\cdots,N$, and $j \neq i$, go along from the fourth step to the fifth step;
4) For $k = 1,2,\cdots,N$, and $j \neq k$, $i \neq k$, go along the fifth step;
5) Update U_{jk} and r_{jk}, While $U_{ji} + U_{ik} < U_{jk}$, set $U_{jk} \leftarrow U_{ji} + U_{ik}$, and set $r_{jk} \leftarrow i$.

The process of the algorithm begins from $U^{(0)}$. First set $U_{jk}^{(0)} = d_{jk}$, then take $i = 1$ as the middle node, $U_{jk}^{(1)}$ is the shortest routing from j to k. When node $1,2,\cdots,N$ are all the middle nodes, then matrix $U^{(N)}$ takes on the shortest routing from j to k, denoted as $U_{jk}^{(N)}$. Perform the iterations according to equation (2):

$$U_{jk}^{i} = \min(U_{jk}^{(i-1)}, u_{ji}^{(i-1)} + U_{jk}^{(i-1)}) \quad (2)$$

Then the distance matrix $U^{(i)}$ and the follow-up node $R^{(i)}$ can be obtained successively. When the value of the distance matrix is converged, then $U^{(N)}$ will be the shortest routing distance-matrix, and $R^{(N)}$ will be the middle-node matrix through which the shortest-distance (between any two nodes) router has passed, i.e. the router matrix.

4.2 Solutions for Reliability Requirement

In the respect of solving the reliability of the Internet service, network service providers show more and more enthusiasm for the application of network stream-control equipment in the redundant structures, i.e. redundancy topology scheme for network exchangers. Conventional practice is to configure them in the main-standby mode, that is, one server is in working state, and the other is on standby. Although such a structure can improve the reliability of the network station by elimination of single-point failure, providers of network service still think that it doesn't take full advantage of the resources, for the standby server keeps in an idle state and will not take over the network service unless the working server breaks down.

Presently, providers of network service require that network equipment manufacturers build a new redundant structure for them. In this new structure, all equipment could deal with network fluxes, so that the throughput of the network station would be increased and the response time of users shortened. Therefore the ITEF has brought forward the concept of Virtual Router Redundancy Protocol (VRRP). The VRRP technique has provided a highly reliable solution for the application of the Internet-based fire remote monitoring system. And it has also eliminated single-point failure over the whole system. For example, the Alteon switch based on the VRRP technique could set up a very sound platform for the system, and could cope with various situations such as server load balancing, firewall load balancing, etc. Furthermore, the Alteon Switch could detect the router fault and switch it in just one second.

4.3 Solutions for Security Requirement

Currently attacks of network "Hackers" and propagation of ruinous virus are the main menaces which threaten the security of the network. As for the Internet-based fire remote monitoring system, special-purposed virtual network technique should be used to ensure the security of the information. With the special-purposed network established, the data can be transmitted on the Internet via the secured "encrypted route"[5]. The operation system for the server and the client should use the Windows XP with a higher level of safety. Moreover, installation of firewall, invasion detecting system and virus-defense software, along with the adoption of access control technique and ID verification technique, is also necessary.

A firewall is considered as the first defense barrier in protecting private information. To achieve greater security, data can be encrypted, and the system can be designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet will pass through the firewall, and the firewall will examine each message and block those that do not meet the specified security criteria.

In practice, the firewall of the fire remote monitoring system should use two or more techniques, such as packet filter, application gateway, circuit-level gateway, proxy server etc.
In addition, in order to ensure the security of the fire monitoring system, it is necessary to enhance the network management. Appropriate system management can decrease the insecurity of the network to a minimum level.

5. CONCLUSIONS

Through reconstruction of the current system at a low cost, the Internet-based fire remote monitoring system can resolve lots of problems about remote monitoring of fires, and also can improve the availability and efficiency of the system greatly. It is highly advantageous for the fire department to supervise the fire alarm equipment in a unified mode and make judgment of the fire situations in the shortest time. It conforms well to the developing trends of the fire auto-alarm system, and will enjoy a promising market and widespread application in the near future.

REFERENCES

[1] *A Resource Allocation Model for QoS Management*, Ragunathan Rajkumar, 1999, http://www.cmu.edu
[2] W Richard Stevens. *TCP/IP illustrated volume 1: the protocols*. Beijing: China Machine Press, 2000
[3] UYLESS BLACK.*IP Routing Protocols; RIP, OSPF, BGP, PNNI & Cisco Routing Protocols [M]*. Beijing: Publishing House of Electronics Industry, 2000.
[4] Tang Baomin, etal, *the Base of Telecom Network Technique*, Beijing: Posts & Telecommunications Press Pub, 2001, (In Chinese).
[5] Chen Tao, "Virtual Private Dial Networks Technical," *Journal of Communications Today*, No.2, pp.6~7, 2003 (In Chinese).

Hongwei Zhu is an engineer in Department of Fire Command, the Chinese People's Armed Police Force Academy. He graduated from Chongqing Communication Institute and got the master's degree in 2003. His research interests are in fire auto-alarm system, communication and network security.

An Efficient IDS Algorithm Based on Alarm Correlative Analysis

Yingzhan Kou, Sumin Yang, Lijun Chen, Hongfeng Lu
Department of Computer Engineering, Ordnance Engineering College
shijiazhuang,Hebei, 050003,China
Email: ysmyxh@tom.com

ABSTRACT

The validity and real-time characteristic of alarm analyzing is two important factors of IDS. In the paper, an efficient algorithm named IDS_ACA (IDS based on Alert Correlative Analysis) is proposed which improves the efficiency of correlative analysis by three ways. Firstly, the correlative border value is increasing by defining an interval time value. Secondly, the speed of correlative analysis is improved by the way of transferring correlative analyzing to searching analyzing. Thirdly, the searching efficiency is improved by two grade analyzing approach for correlation. Based on the description of the proposed algorithm, experimental results are given, which show that this algorithm can analyze the alarms both efficiently and accurately.

Keywords: Alarm, IDS, Correlative Analyzing, Hash Table, Searching Analyzing

1. INTRODUCE

The main function of the firewall technology is to check the network communication at the network entrance and refuse outside illegal IP address by filtering source address, which is an effective way to prevent the unauthorized host from visiting so as to minimize the possibilities that the system might be attacked. Under the limitation of firewall's capability, it can't provide run-time intrusion detective ability, so the association between firewall and intrusion detection [1] has become the most effective resolving scheme for the current network security. At present, the process of the alarm analyzing is performed by following ways: (1) According to the similarity of characteristic among alarms, the alarms are analyzed by the correlative means [2], but the effect of which depends on the validity of attributes that the experts choose. As a result, we can not find out the cause and effect connections among alarms, and to definite the similarities among alarms, and to screen out the effective similar characteristic values from these attributes. (2)The machine learning method [3] is adopted to learn the implicit correlative mode of the alarm data and to analyze the newly produced alarm data by the learned alarm correlative mode, which can generate alarm correlative mode automatically. However, it needs a large mount of data training, and it is impossible to analyze the correlative mode beyond the training data. Moreover, the machine learning method is not very mature, on the one hand, the learning results is not very ideal, on the other hand, it is very difficult to screen out the training data, so we need to include more correlative modes. (3) A result analyzing device is adopted[4,5], which is a kind of mechanism with hierarchy correlations. Firstly, correlative analyzing to alarms can be carried out according to the attribute characteristic of alarms, and the correlative alarms can be analyzed by the certain correlativity between pre-defined alarm and other alarms. This way is similar to the detective mechanism of IDS misused characteristics. But this method can not offer enough information to possible correlative alarms and can not judge the course that the attackers organize the entire movement of attack. As a result, it is rather difficult to choose the correlative characteristic information, and to define the relations among the alarms because of not foreseeing the whole attacking course.

Otherwise, the correlative technology has achieved quite great progresses as the best optimized combination of the overall network security strategies, although by associate technology we can not guarantee absolute safety, the firewall can monitor the visit activities from external networks to internal networks completely, take detailed note and educe the suspicious attack by analyzing the note. So in the paper an efficient IDS algorithm based on alarm correlative analysis, which improves the speed of alarm analysis by defining an interval time value, and transferring correlative analyzing to searching analyzing, and two grade analyzing approach for correlation.

The paper is organized as follows：In section 2, we discuss the existing main problems of alarm correlative analysis. In section 3, we propose our new scheme and analyze the reasons and ways to improve efficiency in detail, the experimental results to assess the performance of the proposed algorithm are presented in section 4, and some characteristics and discussions are highlighted, and finally concluding remarks are given in section 5.

2. THE EXISTING PROBLEMS OF TRADITIONAL IDS CORRELATIVE ALGORITHM

During the process of association between IDS and the firewall, the firewall is the correlative centre and it provides the interfaces to IDS for transferring. However, whether adopting the association or adopting what kind of association depend on the IDS itself. Therefore, the current existing problem of IDS affects the associating of IDS. At present there are several problems in the course of IDS associating as follows:

(1) Lack of a standard correlative protocol. Some of the current used protocols of the association are all doing things in their own way and haven't become the standard or criterion in the industry.
(2) The association happens mainly between one IDS and a firewall, though some IDS may associate with a firewall at the same time, but there is no connections among these IDS which lack of corporation.

At present, because of high false-report rate of IDS, IDS may send wrong correlative information to the firewall. On the one hand, the non-harmful data may make the firewall be over loading, on the other hand, it may make the firewall take wrong action and affect user's normal work.

Because of the limitation of IDS itself, the faulty detective mechanism is apt to cause failing to report, which brings the problem of realizing the correlative function.

3. THE EFFICIENCY ANALYSIS OF IDS_ACA ALGORITHM

3.1 The Definition of HyperAlert

Definition 1: HyperAlert type is a ternary array T =(fact, prerequisite, consequence).

Where **fact** is a group of attribute names. Each attribute has its certain value range. **Prerequisite**, whose freedom variables are all included in **fact**, is a logical formula of a group of predicates which is used for a predicate description to the essential condition of that type of successful attacking; **consequence** ,whose freedom variables are all included in **fact**, is a logic formula of a group of predicates, too. This attack type has an effect on the latter attack, which is described by the group of the logic formula.

Every **HyperAlert** type provides a description to a kind of attack type. **Fact** provides some attribute information of attack detected. The value of the logic formula of predicate is true, which is the essential condition of successful attacking provided by **prerequisite** .The successful attacking having effect on the latter attacking, which is described by **consequence**, is that the value of the logic formula of predicate is true.

3.2 The Efficiency Analysis of The Proposed Algorithm

The main problem of correlative analysis is the efficiency of analyzing. This paper dissertated how to improve the efficiency of correlative analysis from the following three respects.

- Increasing the correlative border value.

The purpose of **HyperAlert** correlative analysis is that as to every **HyperAlert** instance produced, **HyperAlert** correlative analysis can analyse whether or not another **HyperAlert** instance is prepared for its producing, namely the essential condition . Consequently,it is needed to compare one **HyperAlert** instance with another. In this way, if a large number of **HyperAlert** instances are produced ,the analyzing expenses will be very large. If the number of **HyperAlert** is **n**, it will need to compare **n *n** time, such analyzing efficiency will inevitablely be very low.

Therefore, in order to improve the efficiency, we have made the following definition: If the **HyperAlerts** are produced in very close time, there will be correlative relationships among them, otherwise, no relationship exist. We define an interval time value **T**, if the time interval between two **HyperAlerts** is within **T**, we will deal with them correlatively. But the one that is needed to pay special attention to is that the value of **T** should be moderate. If the value is partially big, the efficiency of correlative analysis will be low; if the value is partially small,it will be not easy to find the correlations of the alarm.

- Transferring correlative analyzing to searching analyzing

It is one aspect that we adopt time interval value to improve the speed of correlative analyzing for **HyperAlert**, however, it can't solve the efficient problem. According to the data type characteristics of **HyperAlert,** we can improve the analyzing efficiency by transferring correlative analyzing to searching analyzing.

As in the establishment of knowledge database, we have add all the cause and effect correlative relations among the **HyperAlert** types into it. So with the help of the knowledge database we can correlate all the correlative **HyperAlert** instances. So long as we compare that whether the first generated consequence of **HyperAlert** has the same predicate logic as the latter prerequisite of **HyperAlert** or not, (the first and latter one means that the **end_time** of **HyperAlert** should be smaller than the **begin_time** of prerequisite in **HyperAlert** instances) we can assert that whether the two **HyperAlerts** have cause and effect correlative relations or not.

As the IDS alarm that the IDS analyzing center receives comes from each IDS, so it is necessary to synchronize the time among each IDS. Therefore, we define that the reporting and transmitting of IDS alarm is divided by the generating time sequences, that is to say that the HyperAlerts are ordered by the timing ascending sort . So we needn't consider about the time order of HyperAlert when making correlative analyzing.

- Two grade analyzing approach for correlation

When analyzing if two kinds of **HyperAlert** instances have related relations on the basis of finding the analyzing arithmetic, we should analyze whether these two types of HyperAlert have related relations in the knowledge base at first, that's to say analyzing whether the consequence's predication of one **HyperAlert** are the same as the prerequisite's predication of the other **HyperAlert** or not, and if they are different with each other, we can recognize that they are not correlative, otherwise, we may consider further that whether their parameter are the same with each other or not, if they are, then they are correlative, it will improve the searching efficiency with this correlative method.

Based on the design of the alarm analyzing arithmetic above, we design the two level hash data structure to perform the correlative analyzing and storage for the alarm.

The first level hash is build on the predication of predicative logic, which is to locate the storage location of the alarm for the first time, as the predication is static and the number of them are limited, so the length of the first level hash table are equal to the kind count of the predictions, besides, the first level hash has chain address which is pointed to a hash pail of the second level.

The second level hash is to be built on the parameter of predicative logic, which is to locate the storage location of the alarm for the second time according to the parameter value of the predicative logic. The second level hash adopts hash pail to realize it, the length of it are defined according to the concrete conditions, as to the width of the hash pail, we usually set it three. When computing the hash value of the parameter of predicative logic, alarms who have the same hash value are located these three place by the sequence, every layer of the hash pail has a chain address which pointed to a hash pail whose dynamic generated length equals one.

4. SIMULATION

In order to verify the performance of ACA_IDS, various tests were performed between it and the algorithm of Lane T.[6] with data KDD CUP99. Table1 list the comparative results:

Table 1. the result of the different algorithm

Size of Data set	Comparative attribute	IDS_ACA	Lane T.'s
1000	Run time	10 second	90 second
	True alarm	60%	20%
	False alarm	0.2%	0.8%
2000	Run time	25 second	210 second
	True alarm	90%	85%
	False alarm	0.35%	0.4%
3000	Run time	40second	450second
	True alarm	91%	89%
	False alarm	0.2%	0.8%

From table 1, we can see that the performance of the proposed algorithm is much better than other algorithm. The accuracy and speed of true alarm and false alarm analysis is improved evidently. By comparison with Lane T.'s algorithm, the run-time is improved almost 10 times. The two major reasons are as follows: On the one hand this system builds the knowledgebase, which can describe the causality of the alerts. By means of correlating all the alerts of IDS linked with firewall, the false alerts of the IDS can be eliminated and decreased, which will improve the accuracy of the linkage system. On the other hand, because this system uses two-level hash structure to correlate alerts of IDS, Its highly punctuality ensure that the alert can be correlated in time.

5. CONCLUSIONS

A novel IDS algorithm based on alarm correlative analysis is proposed in the paper. It not only has virtue as well as traditional IDS correlative algorithm, but also improves the alert analysis, including frequency and trend by three means. By IDS_ACA algorithm, administrators can make quick response for each anomaly situation. The experiments have proven its effectiveness also.

REFERENCES

[1] Mukherjee B, Heberlein L T, Levitt K N. *Network Intrusion Detection [J]*, IEEE network, 1994,8(3):26-41.

[2] Peng Ning, Sushil Jajodia, Xiaoyang sean wang, "abstraction-based intrusion detection in distributed environment", 2001.

[3] Sinclair C, Pierce L, Mataner S P. "An application of Machine Learning to network intrusion Detection [C]", Proc. of *the 15th annual computer security application conference*, 1999.

[4] P. Ning and Y. Cui, "An intrusion alert correlator based on prerequisites of intrusions", Submitted for *publication. Available as Technical Report* TR-2002-01, Department of Computer Science, North Carolina State University, January 2002.

[5] Peng Ning and Dingbang Xu, "Adapting Query Optimization Techniques for Efficient Intrusion Alert Correlation", Department of Computer Science North Carolina State University Raleigh, NC 29695-7534, August 2002.

[6] Lane T. *Machine learning techniques for computer security domain of anomaly detection[D*], purdue university, 2000.

[7] H. Debar and A. Wespi, *Aggregation and correlation of intrusion-detection alerts*, In Recent Advances in Intrusion Detection, LNCS 2212, pages 85-103, 2001.

[8] A. Valdes and K. Skinner, "Probabilistic alert correlation", In *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001)*, pages 54-68, 2001.

[9] F. Cuppens and A. Miege, "Alert correlation in a cooperative intrusion detection framework", In *Proc. of the 2002 IEEE Symposium on Security and Privacy*, May 2002.

[10] S. Chandrasekaran, M.J. Franklin. "Streaming queries over streaming data", In *Proc. of VLDB*, August 2002

[11] A. Valdes, K. Skinner, "Probabilistic alert correlation", *Workshop on Recent Advances in Intrusion Detection*, pp.54-68, 2001

[12] C. Rocha, et.al., "A hybrid approach for searching in the semantic web", Proc. of *the 13th Conf. on World Wide Web*, pp.374-383,2004.

[13] B. Aleman-Meza, C. Halaschek, I. B. Arpinar, A Sheth, "Context-Aware Semantic Association Ranking," *Proceedings of the FirstInternational Workshop on Semantic Web and Databases*, Berlin, Germany, September 7-8, pp. 33-50, 2003.

Yingzhan Kou is currently full professor in Department of Computer Engineering, Ordnance Engineering College. He received the B.S. degree in computer science from Ordnance Engineering College in 1985, and M.S. in computer science and information engineering from Beijng Institute of Technology, china, in 1993. Now he works in Department of Computer Engineering, Ordnance Engineering College.His research interests includes network security, software engineering, image processing and adaptive computing.

.

Sumin Yang received M.S. in computer science and information engineering from Xi'an Ploytechnic University, Xi'an, shanxi, china, in 1996. Since then, she works in Department of Computer Engineering, Ordnance Engineering College, where she is currently working towards the Ph.D. degree. Her research interests include wavelets, network security, image processing and digital watermarking.

Solving TSP Based on A Modified Genetic Algorithm*

Wushi Dong, Shasha Cao, Niansheng Chen
Department of Computer Science, Hubei Normal University, Huangshi,Hubei 435002,China
Email: hschenns@163.com

ABSTRACT

The edge recombination crossover is firstly put forward by Whitley. This kind of crossover operator mainly emphasizes the adjacent relationship among the genes (cities) on chromosome (return route). However, it only considers adjacent relationship and ignores the quality of such adjacency. Thus a modified edge recombination crossover is put forward in this paper. By recombining the shortest edge, the edge recombination crossover (ERX) is changed into the short recombination crossover (SERX), which can transmit the adjacent relationship of good quality to the next generation. The SERX shows its better convergence and optimization performance.

Keywords: Genetic Algorithm；Traveling Salesman Problem；Short Edge Recombination Crossover

1. INTRODUCTION

TSP is an NP complete problem, its solving has a great value in computation theory and practical application, and presently, genetic algorithm is the most effective method of solving TSP. Aiming at solving TSP by genetic algorithm, many researchers have put forward diverse modified methods: The viewpoint in Ref.[1] is the diversity of groups could be guaranteed by the consistency control method. The viewpoint in Ref.[2] is that generating of the outstanding model and speed of the algorithm convergence rate should be accelerated by the immune genetic algorithm. The viewpoint in Ref.[3] is that a crossed, variant parallel processing control method is instructed according to the contradiction between the speed of convergence and the diversity.

Aiming at solving TSP, various genetic algorithms always rely on coding of the problem and genetic operation operator. The crossover of genetic operators is taken as the key for the development of genetic algorithm because of its great effect on the algorithm’ s quality. At present time, the research on crossover tends to include illuminating information [1], so the son generation can inherit the information of edge in farther generation. For example: As Ref.[1] has said, a good effect is gained by using the Greedy Crossover(GX). As Ref.[4] has shown, the performance of Insert Crossover(IX) is better than that of the large scale TSP. As Ref.[5] has shown, the performances of both Two-change Illuminating Crossover and Three-change Illuminating Crossover are better than that of the symmetrical and asymmetrical TSP. However, as Ref.[6] has said, the Classic Edge Recombination Crossover embodies a great priority at this point, and it has some flaws because its not consider the quality of edge information during inheritance. As Ref.[7] has said, an Illuminating Edge Recombination is designed by combining with Illuminating Crossover and Edge Recombination Crossover. According to the flaws of Edge Recombination Crossover, this paper puts forward Short Edge Recombination Crossover(SERX), making the Illuminating Crossover integrates directly with the operation of Edge Recombination Crossover, so it enjoys a better convergence and optimization performance.

* Supported by the National Natural Science Foundation of Hubei Province under Grant No. 2004ABA023; The Grand Research Project of Hubei Province Department of Education in China under Grant NO. D200622003.

2. TSP DESCRIPTION

TSP can be described as the distances among several cities known, a salesman who has to visit all of the cities, and each city can be visited only once, at last, he must return to the city which he starts his trip. A good arrangement of visiting orders for these cities can make the total trip shortest.

Definition 1: Assuming Diagram G= (V,E), V stands for vertex set, E stands for edge set, and assuming D stands for the distance matrix formed by distances between vertex i and vertex j, so D can be expressed as (1):

$$D=\begin{bmatrix} d(1,1), d(1,2), \ldots, d(1,n) \\ d(2,1), d(2,2), \cdots, d(2,n) \\ \vdots \\ d(n,1), d(n,2), \ldots, d(n,n) \end{bmatrix} \quad (1)$$

Definition 2: Assuming a visiting order $T=(t_1,t_2,\cdots,t_n)$ to cities $V=\{v_1,v_2,\cdots,v_n\}$, and $t_i \in V(i=1,2,\cdots,n)$, so the mathematical model of TSP can be expressed as (2):

$$\min f(T)=d(t_n,t_1)+\sum_{i=1}^{n-1} d(t_i,t_{i+1}) \quad (2)$$

TSP is the method to find the shortest way that passes all of the vertexes and each vertex is passed only one time.

3. THE GENETIC ALGORITHM for TSP

Genetic algorithm is based on coding style, this paper adopts natural coding style that can be understood and operated easily, it’ s the order arrangement of each city including in circuit trip route. For example, individual coding $T=(t_1,t_2,\cdots,t_n)$, ($t_i=1,2,\cdots,n$) means the circuit route starts in city t_1, passing $t_2,t_3,\cdots,t_n$, and at last back to city t_1.

Fitting degree is the standard for evaluating the quality of individuals, the probability of the individual to be inherited to the next generation group can be sure according to its value. According to the improvement of searching for the shortest route, the fitting degree function value is the reciprocal of objective function (the length of circuit route).

Option operation is based on the evaluation of individual’ s fitting degree. This paper adopts Proportional Model, it’ s a kind of backing random sampling method.

Variation is to change the genes of individual randomly at one or many points in minor probabilities. In order to guarantee the diversity of group, and avoid premature convergence, this paper adopts shift variation crossover to mutate, its basic

process is that each individual generates a substring randomly, and then inserts it to a random location.

3.1 Crossover and It's Improvement

The main idea of Edge Recombination Crossover puts emphasis on the adjacent characters' inheritance among the genes (cities) in the individuals (routes). But it only considers for the adjacent characters' inheritance between the cities in the crossed individuals, it fails to judge the adjacent characters. Aiming at this flaw, this paper proposes Edge Recombination Crossover which can judge the adjacent characters during the operation and choose the adjacent characters of good quality to inherit, so it shows its better convergence and optimization performance. The implementation procedure of Edge Recombination Crossover is as follows:

Step 1: Deciding each city's adjacent cities table Pk (right adjacent cities table for not symmetrical, and the last city adjoins the first one) from circuit route Tx and Ty, $k = 1,2,\cdots,n$.

Step 2: Setting the starting city as $Tx'[1] = Tx[1]$ for the new circuit route Tx', and setting counter i=1.

Step 3: Assuming $t = Tx'[i]$, and delete t from all of the adjacent city tables $Pk(k = 1,2,\cdots,n)$.

Step 4: Picking one city c from the adjacent city tables $Pt = \{tj\}$ according to t, and making sure $d(t,c) = \min\{d(t,t_j)\}$ ($t_j \in Pt$). If Pt is null, picking one city c randomly from the cities which haven't been picked, and making it be the city $Tx'[i+1] = c$ which the new circuit route Tx' will visit next.

Step 5: Modifying counter as $i = i+1$. If $i = n$, the new circuit route has been set completely, turning to step f to create a new circuit route Ty',Else, turn to step c to decide the next city in new circuit route Tx'.

Step 6: Substituting Ty for Tx, and still working from step 1 to step 5, another new circuit route Ty' can be decided completely.

A symmetrical TSP which includes six cities is adopted to explain the implementation procedure. Assuming the six cities named 1,2,3,4,5,6, and distances among them are as table 1.

Table 1. Distances among six cities

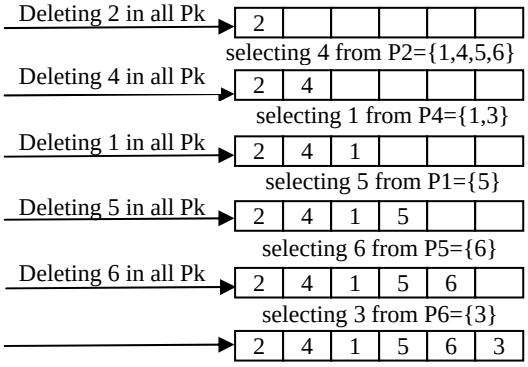
	1	2	3	4	5	6
1	0	5	3	7	8	1
2	5	0	5	1	6	4
3	3	5	0	9	6	7
4	7	1	9	0	1	3
5	8	6	6	1	0	2
6	1	4	7	3	2	0

Two circuit routes Tx and Ty are given:

Tx = (2 4 3 6 5 1)

Ty = (4 1 5 2 6 3)

The procedure of using Short Edge Recombination Crossover to create son Tx' is as follows:



3.2 Flowchart of Serx Algorithm

This paper, in order to avoid convergence in local optimization during the algorithm which isn't the global optimization [8], has proposed operating genetic procedure circularly in finite times, where the initial group is newly created in each generation, and the optimization result of each generation is picked as the best. The flowchart of the algorithm is as Fig. 1.

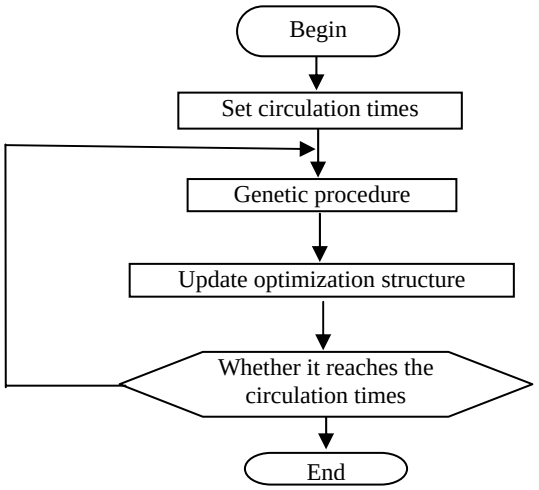


Fig.1. Flowchart of the genetic algorithm

4. EXPERIMENTS AND RESULT

For comparing and analyzing the performance of the SERX algorithm, results of the SERX algorithm and the traditional ERX algorithm and TSPLIB experiments have been compared, and all the experiment data are provided from TSPLIB (http://www.iwr.uni-heidelberg.de/groups/comopt/software/TSPLIB95/tsp/) , and all the algorithms have been programmed with C++ language and run in a PC with Pentium 4.

Definition 3: For the sake of doing analysis conveniently for simulation experiment, optimal ratio α is defined as (3):

$$\alpha = \frac{lt - l}{lt} \tag{3}$$

In which, lt is the optimization provided by [9]. Obviously, when $\alpha > 0$, simulation experiment result is better than the optimization provided by [9], and the bigger α is ,the higher optimization it is, When $\alpha = 0$, simulation experiment result equals with the optimization provided by [9],When $\alpha < 0$, simulation experiment result is worse than the optimization provided by [9], and the smaller α is ,the lower optimization it is.

The examples such as burma14, ulysses16, ulysses22 and bays29 are selected in the experiment of this paper. During algorithm experiment, the loop iterative times is 200. The parameters are set as follows: PopSize=50, Pc=0.80 (cross probability) and Pm=0.08 (modified probability).

In Table 2, according to the experimental result of burma14, ulysses16, ulysses22 and bays29, the SERX algorithm and ERX algorithm and TSPLIB base is shown. It could be found that the optimal solution which used by SERX algorithm is better than which used by TSPLIB. With the increasing of the scale of TSP, the optimizing rate is trend to drop, while that of SERX is hold between 0 ~ 0.02. The optimization searching capability of Short Edge Recombination Crossover is obviously better than that of the traditional Edge Recombination Crossover.

Table 2. Experimental results of burma14, ulysses16, ulysses22 and bays29

Example name	TSPLIB (Ref.[9])	ERX		SERX	
		Optimal solution	Optimal rate α	Optimal solution	Optimal rate α
burma14	—	33.14	—	30.88	—
ulysses16	74.10	80.11	-0.0811	73.98	0.0016
ulysses22	75.67	96.12	-0.2703	75.67	0.0
bays29	9291.35	15861.88	-0.7072	9143.98	0.0159

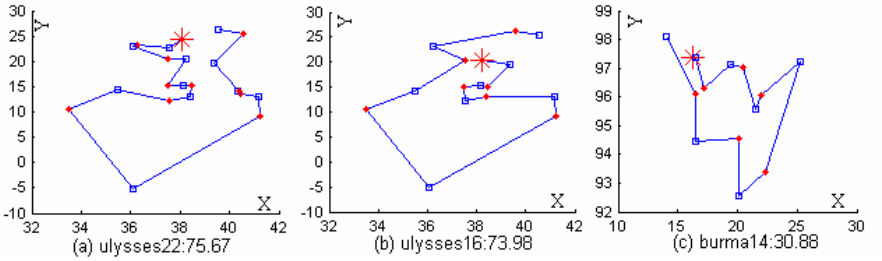


Fig.2. Patrol routes of burma14,ulysses16 and ulysses22

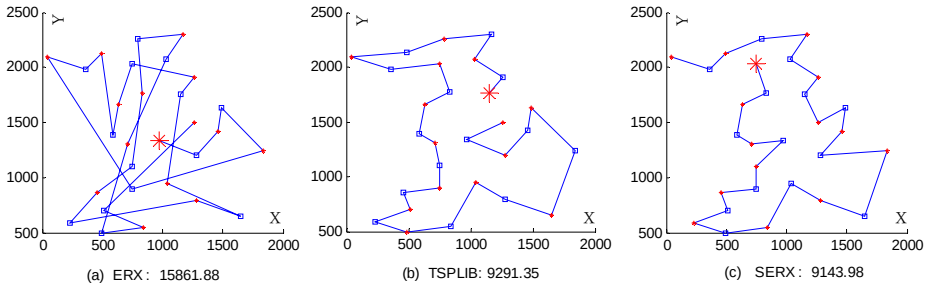


Fig.3. Comparison between patrol routes according to bays29

In Fig.2, the optimal patrol routes which solved by SERX algorithm according to the examples of burma14, ulysses16 and ulysses22. According to the examples bays29, the solution results which used by 3 kinds of algorithms are compared in Fig.3. The patrol routes used by ERX algorithm is shown in Fig.3(a). The optimal patrol routes which adopted by TSPLIB is shown in Fig.3(b). The patrol routes used by SERX algorithm which introduced in this paper is shown in Fig.3(c).

Fig.4 shows the diagrammatic sketch of the convergence rate which used by SERX algorithm during solving bays29. It could be seen that the acceptable convergence rate is achieved by SERX algorithm for this problem.

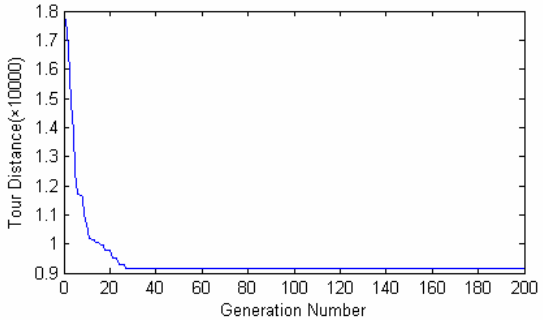


Fig.4. Convergence curve of SERX algorithm for bays29

5. CONCLUSIONS

This paper puts forward the improved SERX algorithm based on the basic theory of Crossover especially ERX in GA algorithm which solves TSP. SERX algorithm has been

implemented with a good optimization performance and rapid convergence speed, it fully considers the design theory of crossover and regards with the genetic characteristic (adjacent relationship among the cities) of TSP and the quality of characteristic (distances among the cities).

The key of using genetic algorithm to solve TSP is how to find the optimization quickly and avoid premature convergence. It can be seen form the genetic procedure above, SERX put forward by this paper can heighten the convergence speed, and the individual can find the optimization quickly, but it would decrease the diversity of the group which leads to trapped in partial optimization point. In order to make up for it, this paper adopts operating genetic algorithm circularly many times, but it increases the time consumption. How to combine GA with other intelligent algorithms (Simulated Annealing Algorithm, Ant Colony Optimization) is the future research problem, which is expect to ensure the population avoid the local optimization to get the global optimization, and prevent premature convergence.

REFERENCES

[1] Xie Shengli, Tang Min and so on, "An improved genetic algorithm for solving TSP",*Computer Engineering and Application*, 2002, 38(8):58-60.

[2] Wang Lei, Pan Jin and so on, *Immune algorithm. Acta Electronica Sinica*, 2000, 28(7):74-78.

[3] Chen Bing, Xu Huazhong and so on, "An improved genetic algorithm and its application in TSP", "Computer Engineering", 2002, 28(9):90-92.

[4] Li Dajun, Zhang Jianwen, Guan Yunlan and so on, "A kind of inserted crossover for TSP", *Computer Engineering and Application*, 2003, 39(33):67-69.

[5] Tang Lixin, "An improved genetic algorithm for TSP",*Journal of Northe Astern University(Natural Science)*, 1999, 20(1):40-42.

[6] Whitley D,et "al.Scheduling Problems and Traveling Salesmen:the Genetic Edge Recombination Operator "[J],*Proc.of 3rd Int.Conf.on genetic Algorithms*, 1989: 133-140.

[7] Wen Jie, Ni qin, "Improving genetic algorithm for solving TSP", *Mathematics in Practice and Theory*, 2005, 35(2):129-132.

[8] Zeng Hongxin, Bing Hongzan, Zhang Fen, "A kind of improved genetic algorithm for multi-variety assembling order",*Journal of Huazhong University of Science and Technology(Natural Science)*, 2006, 34(3):39-42.

[9] http://www.iwr.uni-heidelberg.de/groups/comopt/software/TSPLIB95/tsp/

Time-lapse Seismic Attributes Analysis Based on Parallel Genetic Algorithm *

Qicheng Liu, Yibin Song
School of Computer Science and Technology, Yantai University
Yantai, Shangdong 264005, China
Email: ytliuqc@163.com

ABSTRACT

Reservoir characterization prediction of time-lapse seismic data using seismic attributes is an important technique because it allows extrapolation of reservoir characterization throughout a seismic volume. This study presents a new method for choosing the seismic attribute of time-lapse seismic using a genetic algorithm approach. The genetic algorithm is a desirable method to select the best combination of attributes. Attribute selection using genetic algorithm can choose the optimal number and type of seismic attributes for reservoir characterization prediction. One of the major disadvantages of genetic algorithms is that they are very slow. In this paper we show how the execution time can be reduced by using a commercial shared memory multiprocessor. This work uses the processing power of a network of heterogeneous computers (PCs, workstations, etc.) for the parallel and efficient execution of the genetic algorithms using MPI.

Keywords: Time-lapse Seismic, Attributes Analysis, Parallel, Genetic Algorithm

1. INTRODUCTION

Time-lapse seismic is a rapidly advancing technology, which allows for dynamic reservoir characterization in a true volumetric sense. Using multiple 3D seismic surveys, which are shot at different calendar times, it is possible to deduct valuable information about changes in the reservoir state. The reservoir state is characterized by effective pressure, temperature, and saturation or pore fluid fill. Currently, the main driver for time-lapse 3D seismic is its capability to indirectly measure the saturation. Knowing the reservoir's saturation distribution, hence fluid flow behavior adds tremendous value to and reduces risk in reservoir management. Time-lapse seismic contributes significantly to improved well placement and production strategies. Its value is sometimes limited by the so-called non-repeatability in the seismic experiments.

Time-lapse seismic reservoir monitoring can dynamically image fluid flow change. Successful seismic monitoring depends on a suit of factors, such as reservoir rock and fluid properties, seismic acquisition, processing, and interpretation. So the technology framework of time-lapse seismic includes feasibility analysis, acquisition, processing, and interpretation analysis.

Interpretation analysis begins after repeatability is enhanced through processing. The analysis includes qualitative and quantitative methods. Now, quantitative interpretation has become an active industry research topic. Seismic attribute analysis, including pre-stack and post-stack attributes, is used in quantitative interpretation.

* Natural Science foundation of Shandong Province, China (Grant No. Y2006G22)

Depending on the reservoir, different attributes may exhibit time-lapse behavior. Of these, each attribute may yield different time-lapse responses. Because of the large number of available attributes, a method to select the best combination of attributes is desirable. And an attribute selection method that embodies the non-linearity between attribute combinations and seismic data is desirable.

Genetic algorithm (GA) is a global optimization method derived from the natural process of combination and recombination of the chromosomes in a biological system [1]. Several researchers have reported on geophysical applications of genetic algorithm [2][3][4], but no researchers have introduced genetic algorithm to time-lapse seismic attribute selection. Here, we propose the use of a genetic algorithm time-lapse seismic attribute selection technique. At the same time, several researchers have reported on geophysical applications of parallel technology [5][6], but no researchers have introduced parallel technology to time-lapse seismic attribute selection. Here, time-lapse seismic GA feature selection uses parallel algorithm for the best attribute combination.

2. TIME-LAPSE SEISMIC ATTRIBUTES ANALYSIS

Seismic attributes are used in geosciences interpretation and analysis of 3D seismic data. The successful use of seismic attributes for reservoir characterization is well documented [7] [8]. Seismic attributes are obtained directly from the seismic data. They help to gain insight from the seismic data. For example the "envelope amplitude" represents a measure of the reflection strength.

Since the information content in seismic data is incredible rich in terms of amplitude, frequency, geometry, many attributes have been proposed in the last decade. Seismic attributes represent a mature technology. They are used to help predicting physical properties (e.g., porosity, lithology, bed thickness) of strata being imaged seismically.

Reservoir-based seismic attributes could help delineating anomalous areas of the reservoir, where changes from time-lapse data are evident. Anomalous data areas, in a time-lapse sense, could be indicative of reservoir condition changes. The process of visual inspection of time-lapse seismic can be improved considerably by analyzing multiple attributes simultaneously and by analyzing the resulting time-lapse anomalies in three dimensions. Depending on the reservoir, different attributes may exhibit time-lapse behavior. Of these, each attribute may yield different time-lapse responses. Studying attributes in isolation is not only time-consuming but may also lead to confusing results. For an interpreter it is impossible to study and compare several cubes quickly and in great detail.

Until recently, the choice of attributes for seismic property prediction has been based on prior knowledge of attribute characteristics and cross-plots of one or two attributes versus

the seismic property of interest. Because hundreds of attributes may be easily calculated today, manual selection of attributes is unreasonably time consuming and is not likely to select the best combination of attributes for seismic property prediction. Consequently, automated attribute selection methods are being used to determine an optimal combination of attributes for seismic property prediction.

However, because of the large number of available attributes, a method to select the best combination of attributes is desirable. And an attribute selection method that embodies the non-linearity between attribute combinations and seismic data is desirable.

In our approach, a genetic algorithm (GA) attribute selection technique is employed to combine the different attributes and use their information simultaneously. In the case of time-lapse object detection, we do not know what kind of relationship may exist between attributes and time-lapse anomalies. The GA will be used to optimize the difference between the time-lapse anomalies and the non-repeatable noise

The first step in the process is attribute generation. We generated attributes at certain time intervals for the zone of interest. Then, a GA was used to determine the best attribute combination for reservoir characterization prediction. Finally, Our GA feature selection uses parallel algorithm for the best attribute combination.

3. GENETIC ALGORITHMS APPROACH

Genetic algorithms (GA) are a class of stochastic global search techniques based on biological evolution principles. A GA works simultaneously with a group of different strings (models) called a population. Each iteration of a GA aims to find an optimal model by manipulating this population of Q models using a three-stage procedure of selection, crossover and then mutation. All three stages are controlled by predefined probability values, named probability of selection, Ps, probability of crossover, Pc, and probability of mutation Pm.

Initially applied to machine learning problems [9], it has been applied to many different problems [10] and to a range of geophysical problems. Mitchell [1] explains the GA method in detail and describes a wide range of GA applications with several useful examples. To our knowledge, GA has not been applied to feature selection problems in time-lapse seismic of geophysical applications.

GA feature selection algorithm can be applied to a number of data sets from the machine learning data repository [11]. We modified this approach for the seismic attribute selection problem.

The GA attribute selection technique requires an initial set of attribute combinations. Each attribute combination is termed a chromosome and the entire set of attribute combinations is designated a population. Each chromosome is characterized by a code of zeros and ones with one representing a selected attribute and zero representing an attribute not selected. Each binary digit in the chromosome is a gene. For example, given m total attributes, a population with n chromosomes is represented as a binary matrix, where the selected attributes are ones and the unselected attributes are zeros. A performance index, Pm, and the number of attributes are applied to each chromosome to determine the best attribute subset for reservoir characterization prediction in the population:

$$P_m = (1- R_{val})+ \gamma(A_s / A_a) \quad (1)$$

Here R_{val} is the average cross-validation correlation coefficient, m is a chromosome in the population, γ is the cost coefficient, A_s is the number of attributes in the subset, and A_a is the total number of attributes.

The chromosomes in the population are then compared to each other using tournament selection. Tournament selection randomly selects a predefined number of chromosome pairs. The chromosome with the smallest performance index is chosen from each pair. Next, recombination and mutation operators are applied to the new population of chromosomes chosen by tournament selection. Recombination randomly selects a chromosome pair from the new population and mates the chromosomes based on a predefined probability of recombination. In this study, recombination is accomplished with two-point crossover. The two-point crossover method randomly selects two crossover locations in a chromosome. The information between the crossover locations is exchanged between chromosome pairs. Mutation is then applied to each gene in all chromosomes. For binary chromosomes the mutation operator flips the gene, i.e. if the gene originally was a one, the mutation operator flips it to zero. This entire process comprises one generation. GA training is stopped when either a desired performance index is reached or a maximum number of generations have passed. In either case, the GA training has likely evolved a chromosome that is well suited to the defined problem. In this study, the final chromosome is a subset of attributes that best predict reservoir characterization of time-lapse seismic data.

4. PARALLEL GENETIC ALGORITHM

There are three levels at which the performance of GP may be increased by parallelization as following [12]:

• By fitness case. Every individual in a population is evaluated on every processor, but only a subset of the fitness cases are evaluated on each processor.

• By individual. Every fitness case is evaluated on every processor, but only for a distinct subset of the population.

• By run. A problem will most likely require several runs to produce an adequate solution. These runs can be simultaneous, with each processor evaluating the whole population (for one run) on every fitness case.

Biological mating is highly concurrent! In practice, individuals mate with little regard to the rest of the population. However, many computer simulations of evolution are sequential: the simulation proceeds by sequentially creating a new population as a sequence of mating. The algorithm discussed in this section has been designed for a shared memory multiprocessor. The most obvious target for concurrency is in the creation of the new population, because each mating operation is largely independent of any other. Another source of concurrency is the actual mating operation, which requires independent manipulation on an individual. However, the population size is typically much larger than the number of processors available in shared memory machines, and thus we need only consider the first source of concurrency.

The genetic algorithm can be summarized as follows:

while number of generations<limit & no perfect individual do
  for each child in the new population do

```
      choose two living parents at random from old population
      create an empty child
      for each period of the parents do
         mate corresponding periods
         copy new child period to corresponding position in
         child
      enddo
      repair lost & duplicated labels
      apply mutation to randomly selected period & tuple
      measure fitness of individual.
      if fitness<minimum allowed fitness (based on fitness
         scaling) then
         set child status to born dead
      else
         set child status to living
      endif
   enddo
   old population = new population
enddo
```

The algorithm is viewed from the perspective of the child because this allows random selection of parents. The mating is performed with a randomly chosen cross-over site within the period, and is done for each period of the individual. Mutation is performed on randomly selected periods and tuples, and occurs with some specified probability.

Creation of each child is by random selection of parents, and then random mutation. Instead of one sequential piece of code creating all the children in the new population, a number of workers are spawned and each is then responsible for a fixed number of the children. It is important to minimize inter-process synchronization to maximize the speedup. Since the parents are used in a read-only mode no synchronization is required when the parents are accessed. Further, no synchronization is required on creation of children because each child is created by only one worker, and the new population is only written once within a generation. In a shared memory machine it is possible for the workers to independently write into pre-allocated slots of the new population. Barrier level synchronization is required at the end of each generation.

In order to provide a deterministic execution history, each worker uses a separately seeded pseudo-random number generator. Thus, two executions of the program with the same numbers of workers and the same initial seeds, generate the same result.

5. PARALLEL IMPLEMENTATION VIA MPI

The trend in parallel computing is to move away from specialized traditional supercomputing platforms to cheaper and general purpose systems consisting of loosely coupled components built up from single or multiprocessor PCs or workstations. This approach has a number of advantages, including being able to build a platform for a given budget, which is suitable for a large class of applications and workloads. The jobs that can be broken into multiple tasks that in turn be handed out to individual workers for simultaneous execution, are most suitable for parallel machines.
Recently, cluster of workstations or network of workstations has gained popularity as they provide a very cost-effective parallel-computing environment. Most of these clusters use MPI (Message Passing Interface) as message passing library. MPI calls allow us to communicate and synchronize between the processors. In the present study we have used both MPI and MPI I/O to improve the performance and efficiency of the codes [13], [14].
Conceptually, MPI consists of distributed support software that executes on participating Windows/ UNIX/Linux hosts on a network, allowing them to interconnect and cooperate in a parallel-distributed computing environment. MPI offers an inexpensive platform for developing and running application. Heterogeneous machines can be used in a networked environment. The MPI model is a set of message passing routines, which allows data to be exchanged between tasks by sending and receiving messages.

In the MPI implementation of the modeling codes there is a master task and there are a number of worker tasks. The main job of master task is to divide the model domain into subdomains and distribute them to worker tasks. The worker tasks perform time marching and communicate after each time step. As demanded by the user the snapshot and synthetic seismogram data are collected by the master and written out on the disk.

The main code of MPI for the communication between two adjacent subdomains as following:

```
if(myid>0){
    MPI_Send(&y1[theStart], 1, MPI_DOUBLE,
        myid-1, myid, MPI_COMM_WORLD);
    MPI_Recv(&y1[theStart-1], 1, MPI_DOUBLE,
        myid-1,myid-1,MPI_COMM_WORLD,&status);
}
else if(myid<numprocs-1){
    MPI_Send(&y1[theEnd-1], 1, MPI_DOUBLE,
       myid+1, myid, MPI_COMM_WORLD);
    MPI_Recv(&y1[theEnd], 1, MPI_DOUBLE,
       myid+1,myid+1,MPI_COMM_WORLD,&status);
}
```

6. CONCLUSIONS

The selection of seismic attributes for reservoir characterization prediction is a critical step in any attribute prediction process. The GA attribute selection method presented in this study shows that a number of different attribute combinations can successfully predict reservoir characterization. The variation in GA selected attribute combinations is due to random initial populations of the GA.
Because the genetic algorithms are quite slow to execute, a solution was developed for execution on a parallel processor. Because the process of breeding is inherently parallel, we observed quite good speedups over sequential execution of the algorithm. The implementation of using MPI software system makes network parallel computing easy to implement without knowing the detail of working with a heterogeneous network of computers.

REFERENCES

[1] Mitchell, M., *An introduction to genetic algorithms*, M.I.T. Press, 1996
[2] Yang, J., and Honavar, V., "Feature subset selection using a genetic algorithm: IEEE Intelligent Systems," 13, No. 2, 1998, pp 44-49.
[3] Docherty, P. & Singh, S., "Migration velocity analysis using a genetic algorithm, European Association of Exploration Geophysicists," *Fifty-Seventh Annual International Meeting and Exposition*, Glasgow,

Scotland, 1995.
[4] Mallick, S., "Model-based inversion of amplitude-variations-with-offset data using a genetic algorithm," *Geophysics*, 60, 1995, pp 939-954.
[5] Phadke, S., "2D elastic wave modelling on a transputer based parallel computer: In Supercomputing using transputers," *Narosa Publishing House*, New Delhi, 1994, pp 263-267.
[6] Highnam, P.T. and Pieplrzak, A., "Implementation of a fast, accurate 3D migration on a massively parallel computer," *6lst Ann. Internat. Mtg., Soc. Expl. Geophys*., Expanded Abstracts, 1991, pp 353-356
[7] Gastaldi, C., Biguenet, J., and De Pazzis, L., "Reservoir characterization from seismic attributes: An example from the Peciko Field (Indonesia)," *The Leading Edge*, 16, No. 3 ,1997, pp263-266.
[8] Hart, B. S., and Balch, R. S., "Approaches to defining reservoir physical properties from 3-D seismic attributes with limited well control: An example from the Jurassic Smackover Formation, Alabama," *Geophysics*, 65, 2000, pp368-376.
[9] Goldberg, D.E., Genetic Algorithms in Search, Optimization and Machine Learning, Addinson-Wesley, Reading, MA, 1989.
[10] Holland, J.H., *Adaptation in Natural and Arti_cial Systems*, The University of Michigan Press, Ann Arbor, 1975.
[11] Yang, J., and Honavar, V., "Feature subset selection using a genetic algorithm," *IEEE Intelligent Systems*, 13, No.2, 1998, pp44-49.
[12] Koza JR., *Genetic Programming: On the Programming of Computers by Natural Selection*, MIT Press, 1992.
[13] Bhardwaj, D., S. Phadke and Sudhakar Yerneni, "On improving performance of migration algorithms using MPI and MPI-IO," Expanded Abstracts, *Society of Exploration Geophysicists*, 2000.
[14] Phadke, S., D. Bhardwaj and S. Yerneni, "3D seismic modeling in a message-passing environment," in *Proceedings of 3rd Conference and Exposition on Petroleum Geophysics (SPG'2000)*, 2000, pp 168-172.

Qicheng Liu is a associate professor of School of Computer Science and Technology, Yantai University. He received a B.S. (1992) from Shandong University of Technology, an M.S. (1995) from Shandong University of Technology. He received a Ph. D. (2006) from China University of Petroleum Beijing. His research interests are in information technology of oil exploration, parallel computing.

Automatic Test Toolkits Based on Network

Qinqun Feng [1], Lin Chen [2], Wenfang Yu [3]
[1,3]Computer Application Department, Command Communication Academy,
Wuhan, Hubei Province, 430010, China
[2]Computer Science, Wuhan University of Technology
Wuhan, Hubei Province, 430063, China
Email: nudt92458@yahoo.com.cn

ABSTRACT

After concise introduction of Software test and its significance, An automatic software test toolkits based on network（ATK） is presented in details. Its two departments (Test Server and Test Driver) are described subsequently. Test Server is made up of Test Scripter, Test Data Generator, Test Result Comparator, Test Reporter and other Services, which are based on the Base Type Service (BTS). And finally its advantages, faults are summarized.

Keywords: Software Test, Automatic, Software Test Tool

1 INTRODUCTION

Software testing is the process of executing a program in order to find errors in its source codes and it's accepted widely as a "best practice" for software development. It has been estimated that software testing involves more than 50 percent of software development. It's so expensive, labor-intensive, and times consuming that developer often leaves it out. It's difficult for software developers, project managers and advanced managers to manage and monitor the quality of software with projects becoming more and more complex, and testing consumes an ever-increasing amount of time and resources. Although the investment of software test can be cut down to the lowest level and it can be delayed, the total capital invested will increase in the following procedure. So it's necessary to use automatic software test tools to maintain software procedure, reduce the cost, and use these tools to promote software development. It's a key point to do research on automatic software test tools. Automatic software testing can be an extremely important part of achieving software with high reliability. Manual test is a slow and labor-intensive way and may be insufficient and ineffective.

2 AUTOMATIC TEST TOOKKITS BASED ON NETWORK

Commercial software testing tools are so expensive that the cost of one license maybe be the overall cost of software development. It takes testers long time to understand and get familiar with these tools. The procedure of these tools should be incorporated with the development process. As there are varieties of system environments and developing languages, such as WindowsNT,Windows2000,Unix,C/C++,Fortran and Pascal, Automatic Test Toolkits(ATK) is designed into two departments: Test Server and Test Driver.

Test Server can schedule test cases (or its package) automatically and repeatedly, test reporter can collect the information of test cases, analyze these results and create a reporter and log. The test procedure can be displayed dynamically. The architecture of Automatic Test Toolkits (ATK) is displayed in Fig.1.

2.1 Test Server and Test Driver

Modules of Test server are displayed in Fig.2. It's made up of Result Comparator, Test Scripter, Data Generator, Test Result Reporter, Communication service, Log service, Display service and the Base Data Type service.

Test Server exchanges data between these tested objects, drives these tested objects through the network-based communication service. Test Driver pass the test data, which accepted from the server，to the tested modules after building the link between test server and test driver. One of the powerful features of Test Driver is its ability of isolate, reusing. This feature allows user saving considerable time in generating the test driver program and stub code, which often need for the test.

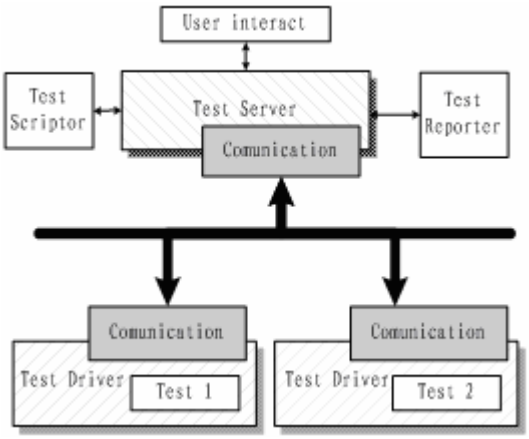


Fig.1. Architecture of Automatic Test Toolkits

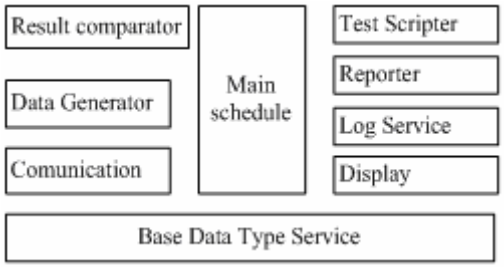


Fig.2. Modules of Test Server

The test process is scheduled by the main monitor of Test Server. At first, test server generates a test case or a test case package using the test scripter, which can be created by any other text editor. The test case drives the test data generator to bring out test data, which will be transferred to the test driver by communication service through network. Test driver loaded the tested modules and input the accepted data. Output data is collected and sent back to test server, which will schedule the comparator to finish the comparison between the output data and the expected value. The result and vital event will be written into the database, which will be prepared for the test record and test reporter.

2.2 Test Scripter

Techniques of generating test cases automatically is very significant as it can reduce the time and cost of testing. Test case's systematic generation using Test Scripter could be automatic. The test case is the description, recorded a test case or its a procedure(or package). It's a text coded by a specific defined script language and is generated by the Scripter. The Scripter is an independent application, and it's embedded in the Test Server. Any text editor can create a script, the Scripter can compile and check it. Test cases are serialized by the test script, and these serialized test cases make up of a test package. The test package includes the input data, output data and expected data.

The following is a test script. It declares an int8 object, generates a group of normal input data subsequently, and then the object sends the test data to the tested module.

```
Int8 var
var.GeneratNormalData;
var.SendData;
```

2.3 Data Generator

Test data used by test cases is generated by an isolated application named Test Data Generator. In order to extend ATK, a data generating container is designed in Test Server, which contains some data generating strategies. The container is maintainable, reusable and extendable. Making a good choice of test data is the key factor of effective test case, the scope of input parameters is determined after analyzes their values and types. The input of these tested units is classified according to the principle of equivalent class, every test data represents a set. The normal value, exception value and boundary value construct the set of input value. The input data enumerate all above types of data. Invalidate input data is eliminated and the clearing of redundant data makes the test be more efficient.

2.4 Test Result Comparator

Test result comparator's main function is getting the difference between output and the expected result, it decides whether the test case is successful or not. The specific comparator method is important to the test system except for these tools operation system provided to check the result. The principle of comparing is clear when the test result is of simple data type, while the comparing principle is complicated as the output data is of complicated style. The comparing method container equips the existing comparator, which overcast static compare and dynamic compare of the simple data type, users can custom or reinforce their own comparators.

2.5 Test Reporter

Test reporter can expediently generate test specification and test report after analyzes the collecting test logs, test input/output data. It provides some default test report document templates, and users can custom their own templates, or develop specific test record and report according to test data and these open interfaces. Test Reporter can publish two formats files(doc and html).

2.6 Other Services

The ATK includes others services, such as communication service, log service and display service, all of them are based on the Base Type Service (BTS). The architecture, data description and operations of base type are defined in its parent class, which exhibit a series of Methods, Events and Properties. The data description of BTS is independent of operation systems, which result in that ATK is independent of developing languages and operation systems. These services are parts of ATK and they make ATK run smoothly.

3 CONCLUSIONS

ATK has some merits, such as, it generates test records and reports intelligently and automatically, it's independent of developing languages and operation systems, and it can be easily integrated into other software platforms to promote the implementation of software procedure. Meanwhile, ATK's Test Data Generator can't meet users' requirements fully, and the tactics and methods of data generation need to emend and strengthen.

REFERENCES

[1] Rovert V. Binder,Testing Object-Oriented Systems: Models,Patterns, and Tools,2001.

[2] Stanley B.Lippman,C++ Primer,2006.

[3] David Chappell,Understanding .NET,Addison Wesley Longman,2002.

[4] Feng Qingqun,Research Based on Software Tested Tools of Network,2006,23(1),P133-135.

[5] Sun xin,"VC++ Lucubrate",Publishing House of Electronics Industry,2006.

Qinqun Feng (1973-) is a instructor of Department of Computer Application Technique, WuHan Command Communication Academy, graduated from the National University of Defense Technology in 1992 with specialty of Mechatronic Engineer; research interests are in software engineering and computer application system integration.

An On-Line Searching Method of Gain-Keeping in MTSA

Ling Zhou [1], Jie Chen [2], A. Aghdam[3]
[1]School of Energy and Power Engineering, Changsha University of Science and Technology, Changsha 410076 China.
[2]School of Electronic & Information Engineering, Wuhan Institute of Technology, Wuhan 430073 China
[3]School of Computer Science and Engineering, Concordia University, Montreal Canada
Email:[1]zhouling70@126.com

ABSTRACT

In this paper, a modified two-step algorithm is applied to an optimization problem in which the objective function is a multi-input single-output nonlinear steady-state model an on-line searching method for gain-keeping is proposed. The simulation results show that the method is effective.

Keywords: MTSA, Gain-Keeping, Steady-State Optimization, On-Line, Simulation

1. INTRODUCTION

The method of statistical modeling was usually applied in industrial processes; nevertheless, such kind of model structures could not exactly reflect actual processes and the optimal solutions based on them could not be really obtained with model optimization techniques. Therefore, a method called Twice Step Arithmetic (TSA) was generally adopted. It recursively corrects model parameters through optimizing and controlling inputs on line. Since the parameter estimation is related to the optimization, the model matches up with the actual process only by the difference of inputs and the real optimal results can be obtained . The problem is that the solution is really not satisfactory if the mathematical model of an actual process is unknown. To overcome this defect, Roberts and Williams proposed a modified twice step arithmetic (MTSA) separating the optimal problem from parameter estimation; however, where to choose keeping gain K, which is obtained in practice, have not be mathematically expressed. For the optimal control on line, it is not allowed to choose gain K on the spot. This paper proposes a method of searching and keeping gain K on line and shows the results of simulation on MISO nonlinear steady-state optimization.

2. THE SEARCHING METHOD OF GAIN-KEEPING ON-LINE

The information intercommunion diagram of MTSA is as shown in Fig1, in which

$$\lambda=\left[\frac{\partial^T F(V,\alpha)}{\partial V}-\frac{\partial F^*(V)}{\partial V}\right]\left[\frac{\partial F(V,\alpha)}{\partial \alpha}\right]^{-1}\left[\frac{\partial F(U,\alpha)}{\partial \alpha}\right] \quad (1)$$

used in actual processes; ε stands for the random error existing in the output of system, F* (V) , which generally satisfies the normal distribution with zero as its average value and σ2 as its variance, and the probability density

$$P(\varepsilon)=\frac{1}{(2\pi)^{1/2}\sigma}\exp\left(-\frac{1}{2}\varepsilon^2\frac{1}{\sigma^2}\right) \quad (2)$$

Assume that the estimation of parameter α satisfies

$$y = Y + \varepsilon = a_0 + a_1 x_1 + a_2 x_2 + \cdots + \alpha x_n \quad (3)$$

where Y is the real output of the process. Let the true value of parameter α be α*and

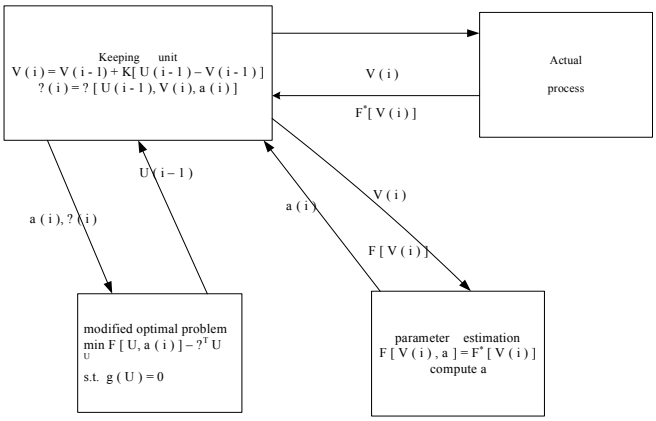


Fig.1. Information Intercommunion Diagram Of MTSA

$$\alpha = \alpha^* + \Delta\alpha \quad (4)$$

where Δα is the difference between α and α*. Substituting Eq. (4) into Eq. (3),we have

$$\Delta\alpha x_n = \varepsilon \quad (5)$$

Eq.(5) indicates the linear relationship between Δα and ε, which implies that Δα also submits to the normal distribution with zero average value and p variance, and its probability density

$$P(\Delta\alpha) = \frac{1}{(2\pi)^{1/2} P^{1/2}}\exp\left(-\frac{1}{2}\Delta\alpha^2\frac{1}{P}\right) \quad (6)$$

In terms of variance,

$$p = M\left[\frac{1}{x_n^2}\varepsilon^2\right] \quad (7)$$

Assuming that every experiment on them be independent and of equal error variance, we have

$$p = \frac{1}{x_n^2}\sigma^2 \quad (8)$$

For the parameter estimation to approach the true value, p must be minimized [3]. Since xn is a nonlinear function of V and the latter is a function of K, p is a nonlinear function of K. Consequently, the solution of keeping gain K becomes to solve the minimum problem as follow:

$$\min_K \; p(K)$$
$$\text{s.t. } K_{min} \leqslant K \leqslant K_{max} \quad (9)$$

where [K_{min} , K_{max}] is the gain interval in which MTSA converges stably. Problem (9) can be solved with one-dimension search.

3. SIMULATION RESULTS

As an illustration example in this paper, the optimal control of formaldehyde is taken as an optimal control model of the actual process[4], in which

$$y = 179372 - 149623.5E - 75839.16/E + 7613568/T + 10373.17/E^2 - 2.545881*10^9/T^2 \quad (10)$$

The original optimal problem is

$$\min_{E,T} \quad y$$

$$\text{opt} \quad \text{s.t.} \quad 635 < T < 672$$
$$0.38 < E < 0.5 \qquad (11)$$

The following model is chosen for the above process:

$$\bar{y} = a_1E + a_2/E + a_3/T + a_4/E^2 + a_5/T^2 \qquad (12)$$

With five pairs of input and output data, the approximate estimation of the initial values of each parameter can be obtained as

$a_1 = -149378$, $a_2 = -75698.75$, $a_3 = 9531392$,
$a_4 = 10353.69$, $a_5 = -3.173778*10^9$.

Modify parameter a_5 by MTSA and meanwhile, add the disturbance signal with zero average value and variance of 2.26 to the output of the object, substitute y for historical y during the iteration and solve the original optimal problem. After 18 iterations, both the optimal input and the objective function are reached, as shown in Table 1and Fig 2.

Table 1 Comparison of the Results

True optimal solution	MTSA solution
E = 0.483	E = 0.484
T = 635.009	T = 635.026

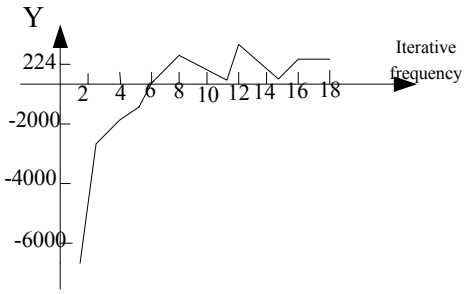


Fig.2. The Value Changes Of The Optimal Object Function During The Iteration

4. CONCLUSIONS

An on-line searching method of keeping gain in MTSA is proposed in the paper. It makes MTSA more applicable to practice by only modifying a single parameter on line, operating simply and actualizing easily. The results of simulation indicate that, when the model or structure of the process investigated is not certain, the true optimal solution can also be obtained. Therefore, it is an effective method of steady-state optimization control on line in the production process.

REFERENCES

[1] P.D. Roberts and T.W. Williams,“ On an Algorithm for Combined System Optimization and Parameter Estimation,” *Automatic*,1981, pp.199 ~ 209

[2] M. Brdys, S. Chen and P.D. Roberts,“ An Extension the Modified two – step Algorithm for Steady -state System Optimization and Parameter Estimation,” *INT J System*, 1986,pp.1229 ~ 1243

[3] W.J. Palm,*Modeling Analysis and Control,*2nd ed,John Wiley & Sons,New York,2000.

[4] R.C. Dorf and R.H. Bishop,*Modern Control Systems,*10th ed,Science Press,Beijing,2005.

Ling Zhou, Sep. 1970, Female, Han nationality, associate professor of School of Energy and Power Engineering, Changsha University of Science and Technology, research interest in modeling and process contrll.

Network Techniques and Applications

Novel Distributed Computing Techniques for Mobile Telecommunications

Souheil Khaddaj[1], Bippin Makoond[1,2], David CC Ong[1], Radouane Oudrhiri[2]
[1]Faculty of Computing, Information Systems and Mathematics, Kingston University, London, KT1 2EE, UK.
[2]Systonomy Ltd, Southbank House, Black Prince Road, London SE1 7SJ, UK.
Email: bippin@systonomy.com, david.ong@bcs.org, S.Khaddaj@kingston.ac.uk, radoune@systonomy.com

ABSTRACT

This paper presents a novel distributed technique based on the application of InfiniBand technology over the RDMA channel Interface to develop a distributed Service Level Agreement (SLA) and enforcement solution for the generalised mobile messaging infrastructure. The paper reports on the construction of a distributed SLA application that is able to handle extremely high throughput and still provide the required data integrity. We developed an SLA quota management model, deployed across distributed servers that provide a comparison illustrating the aftermath of deploying the SLA enforcement solution over InfiniBand and Ethernet technologies respectively.

Keywords: SLA (Service Level Agreement), InfiniBand, RDMA (Remote Direct Memory Access), MPI (Message Passing Interface), Distributed Systems.

1. INTRODUCTION

With the worldwide installed base station of mobile phone owners expected to exceed 2 billion people this year and with most new mobile phones doubling as portable PCs, internet terminals and Telecommunication convergence with IP, Telecommunication operators are urgently looking for alternative solution to accommodate the expected surge in mobile services. There is now a paradigm shift in the methods of engaging the problems and complexities of the telecommunication domain. Using traditional monolithic architectures, the threshold has been reached. Decision makers are looking at understanding and integrating alternative design concepts. This has led to the investigation and adaptation of Parallel Computing, Multi Agent Systems and Distributed Systems to the problem of Telecommunications. The rationale for such a change is firstly because distributed systems provide the flexibility to scale performance, e.g. dynamically adding resources to the solution. Secondly, it provides robustness and multiple nodes redundancy and failover strategies. Thirdly, it provides the flexibility to dynamically allocate resources and distribute resource consumption for efficiency.

The motivating scenarios for our work are situated within the problem realm of the generalized messaging environments. This market consists of Telecommunication operators wishing to grant subscribers and content providers (or consumers) the right to utilise certain resources for some agreed-upon time period. These services use different collaborations between system resources. In analysing the collaborations (resource interactions), we observe that SLA issues can arise at multiple levels. Firstly, operators may agree to enforce the SLA under which resources are made available to consumers [1]. Secondly consumers may want to access and interpret SLA statements published by providers, in order to monitor their agreements and guide their activities. Both providers and consumers want to verify that SLA protocols are applied correctly.

The paper is structured in three sections. The first section describes the distributed computing environment, and the second section describes the business logic, i.e. the SLA counters and conditions. The third section reports on an experiment that has been carried out to benchmark SLA enforcement procedures over InfiniBand against SLA enforcement over Ethernet for distributed systems.

2. THE DISTRIBUTED COMPUTING ENVIRONMENT

2.1 Infiniband Architecture

The InfiniBand architecture is switched-fabric architecture designed for next generation Input Output systems and data centres [2] [3]. The InfiniBand Architecture (IBA) promises to replace bus-based I/O architectures, such as PCI, with a switched-based fabric whose benefits include higher performance, extremely low latency and higher reliability, availability, scalability, and the ability to create modular networks of servers and shared I/O devices. With InfiniBand Architecture, server clusters can be configured for the first time with an industry standard I/O interconnect, creating an opportunity for clustered servers to become ubiquitous in data centre deployments.

InfiniBand technology works by connecting host-channel adapters (HCAs) to target channel adapters (TCAs). The HCAs are located near the servers' CPUs and memory, while the TCAs are located near the systems' storage and peripherals. A switch is located between the HCAs and the TCAs, directing data "packets" to the correct TCA destination based on information that is bundled into the data packets themselves (Fig.1). The glue between the HCA and TCA is the InfiniBand switch, which allows the links to create a uniform fabric environment. One of the key points of this switch is that it will allow packets of information (or data) to be managed based on variables, such as SLAs and a destination identifier.

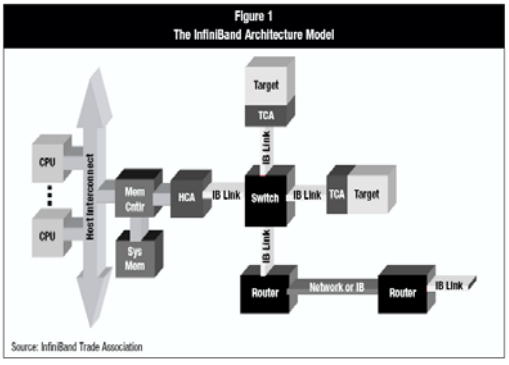


Fig.1. InfiniBand Architecture Model

In essence, the HCA provides mechanisms to send messages and access a remote node memory in high-speed, low-latency, minimum software overhead and direct access from user

applications. These capabilities enable the detachment of the system elements (CPU, I/O, and Storage) in a way that doesn't affect performance, and achieves clustering and linear scalability.

2.2 Software Primitives

In this study we built the SLA Enforcement prototype using MPI-Pro, developed by Verari Systems [4]. MPI-Pro is a complete implementation of the MPI-2 library that supports functionalities such as dynamic process management, one-sided communication, and MPI I/O. The MPI-2 process model allows for the creation and cooperative termination of processes after an MPI application has started [5]. It exhibits the concept of dynamism in distributed communication by providing a mechanism to establish communication between the newly created processes and the existing MPI application [6].

Remote memory operations have been used in a number of applications [7] [8] and MPI extended its communication mechanisms in adopting RDMA to allow one process to specify all communication parameters, both for the sending side and for the receiving side (Fig.2). This mode of communication facilitates the coding of some applications with dynamically changing data access patterns. Each process can compute what data it needs to access or update at other processes. However, processes may not know which data in their own memory need to be accessed or updated by remote processes, and may not even know the identity of these processes. Thus, the transfer parameters are all available only on one side. Regular send/receive communication requires matching operations by sender and receiver. In order to issue the matching operations, an application needs to distribute the transfer parameters. This may require all processes to participate in a time consuming global computation, or to periodically poll for potential communication requests to receive and act upon.

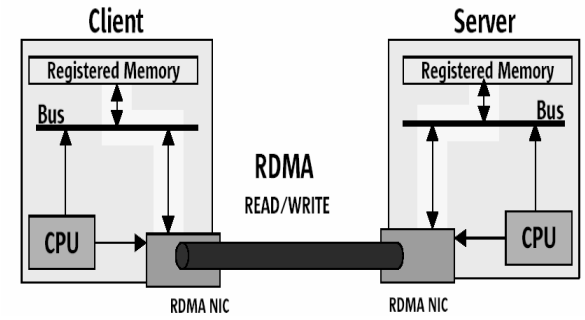


Fig. 2. The Mechanism of RDMA

The use of RDMA communication mechanisms avoids the need for global computations or explicit polling (Fig.3). Message-passing communication achieves two effects: communication of data from sender to receiver; and synchronization of sender with receiver. The RDMA design separates these two functions. Three communication calls are provided: MPI PUT (remote write), MPI GET (remote read) and MPI ACCUMULATE (remote update).

3. THE SERVICE LEVEL AGREEMENT

SLA is a contract between suppliers and clients. In the domain of information systems, the operation and management of SLA requires data integrity. A model of

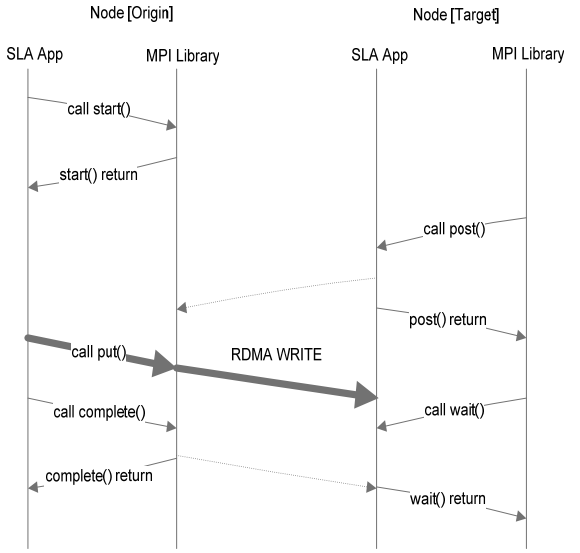


Fig.3. MPI Using RDMA

shared basis for statistical calculations to ensure the integrity of SLA counters represented by times series instances has been reported in [2]. These instances are used as input for several statistical metrics. It is a complex and challenging problem to manage Service Level Agreement (SLA) within an operating environment that comprises of distributed participants and utilizing distributed resources [9] [10] [11]. Allocation and management of dynamic resources that spans across several nodes may become a bottleneck for performance, particularly when applied to large scale wireless messaging systems.

Under the centralised server solution it is possible to throttle message rate for individual clients to prevent system flooding or to control the level of service offered to individual clients. This is considerably harder to develop on a distributed architecture since the client's messages may be spread over a several dispersed nodes. Customers agree for a certain level of service from its providers (SLA). An example of an SLA is the quota of messages a customer is allowed to submit to a system. The quota can be a fixed number (e.g. 1000 messages limit) or a throughput limit (e.g. 50 messages per second). The aim of the work is to provide a model that addresses the problematic of SLA management over a distributed architecture.

Typically the distributed architecture consists of a number of heterogeneous servers. Individual clients may send messages to more than one server. In our case study, there is an obligation to manage their quota across all the servers. Since the system is distributed, the issue of quota control enforcement is more complex; due to the fact that there is no single point of reference. A client may have several accounts and each account has an ID. When a client submits a message, the account ID uniquely identifies the quota limit associated to that client. As message is submitted, the number of messages (balance) is incremented. The counter is updated on all the servers of the distributed systems. This results to all nodes having same counter for each accounts. Thus as messages are distributed across the nodes the counter keeps global tracking of each account/quota.

The distributed SLA solution to enforce a quota management policy flooding is illustrated in Fig.4 which gives a general

view of how the SLA Enforcement application inter-communicates across distributed servers.

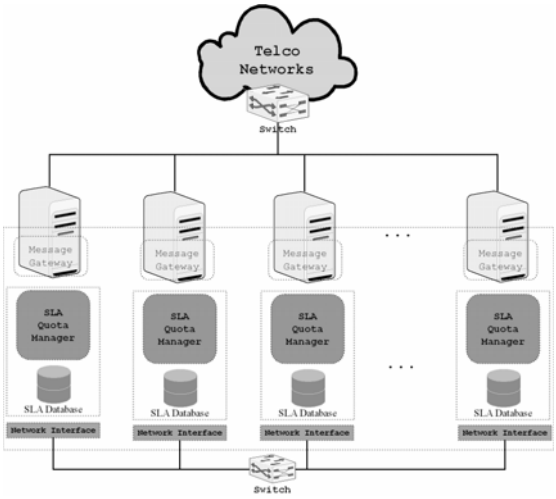


Fig.4. Distributed SLA Enforcement Model

To use the system a client should start by subscribing to the service provider (operator) and opens an account which will allow the client to send messages to the message gateway. The message gateway will then query the SLA Quota Manager to confirm whether the message can be accepted for further processing. The SLA Enforcement Manager consults a cache to validate the message and sends back the appropriate acknowledgement to the message gateway. It increments the balance for that particular account (client) and distribute the update to its neighbours. Each Message gateway on the network receives the update resulting to all the SLA Database to be in sync across the distributed servers.

Fig.5 shows state transitions of the methods of each class. The point of focus is on the change of state triggered by the locking and unlocking mechanism when SLA records are accessed vigorously. Using the state chart, we ensure that a dead lock situation is not reached.

In the next section, we report on this efficient SLA enforcing strategy across several nodes that on the one hand preserve data integrity of the SLA counters and on the other hand perform at high throughput and very low latency that is based on the use of InfiniBand over RDMA channel interface for the deployment of the SLA Enforcement.

4. IMPLEMENTATION AND TESTING

The test exercises will compare the difference in performance and resource consumption in running the SLA Enforcement prototype over IB and Ethernet (Fig.6). The keys HP03, HP04 are the host names of the test servers, and AGT is the Agent which is a series of Java modules specifically developed for shared memory tests over transports such as InfiniBand and TCP/IP. The MPI environment of collective processes is known as a "World". For each AGT node, user input can be injected for various testing scenarios. The AGT itself consists of a Java Interface (JIN), providing the interface and input regulator, and an InfiniBand Adaptor (IBA), providing access to the shared data.

In order to test the system the following SLA attributes are configured:

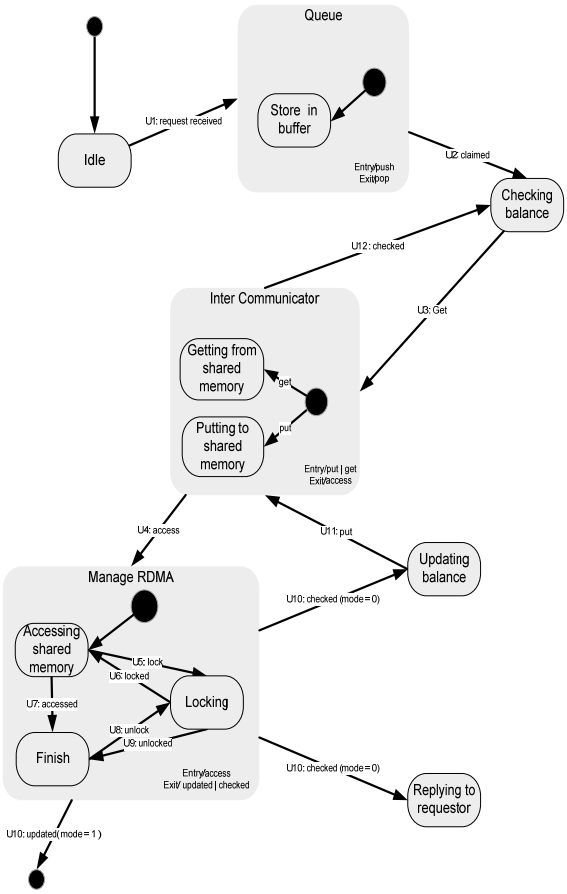


Fig.5. State chart model of SLA prototype

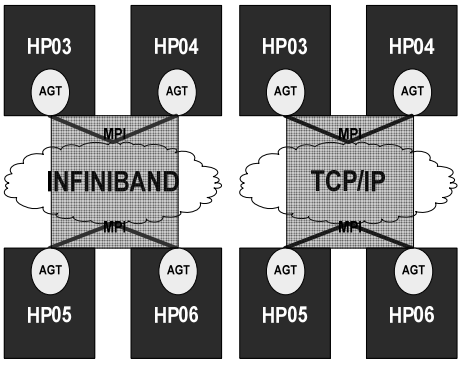


Fig.6. Logical view of the test plan

1. Number of Accounts: 1,000
2. Quota per second per Account: 1,000,000

During run-time CPU utilisation is recorded for the servers and the shared data is checked. The objective is to validate the behaviour of the system against predefined goals:

1) To compare the performance no. of request over time against no. of replies over time between using InfiniBand VAPI protocol and Ethernet TCP IP (transaction /sec) independently.
2) To compare the CPU usage when executing the SLA Enforcement prototype over InfiniBand VAPI against Ethernet TCP/IP.
3) To check the data integrity of the SLA Enforcement prototype as the number of nodes (ranks) increases in the distributed system.

The graph depicted in Fig.7 clearly illustrates that when using InfiniBand VAPI, the CPU usage / consumption is 3 to 4 times less than Ethernet TCP/IP. This is because when TCP/IP packets are transported, they are required to go through the TCP/IP stack which consumes CPU time. Figure 7, also compares the performance of the SLA Enforcement application when deployed on InfiniBand VAPI and Ethernet TCP/IP. The graph addresses the performance as number of transactions per second, i.e. the number of request being replied and the number of updates being published over the shared memory space.

Fig.8 shows a clear gap between TCP/IP and VAPI in terms of performance. The latter out performs TCP IP by a factor of 8. We observe the performance of InfiniBand compared to TCP/IP, and agreed that TCP/IP is nowhere near the speed of InfiniBand. The next quality attribute to be addressed is data integrity which is shown in Fig.9.

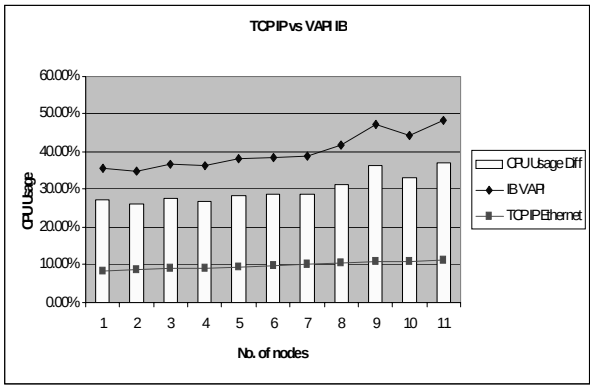


Fig.7. CPU Usage VAPI Vs. TCP/IP

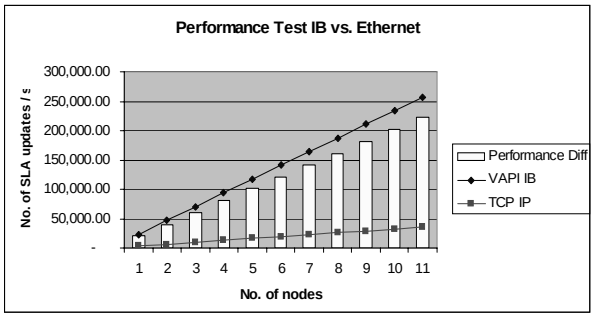


Fig.8. Performance VAPI Vs. TCP/IP

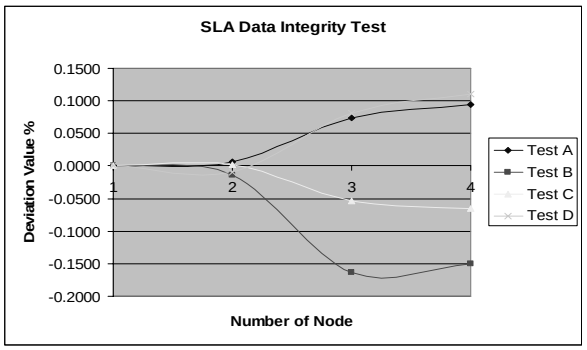


Fig.9. Data Integrity Tests Results

A number of tests were carried out to find out level of accuracy in updating the SLA counter distributed across multiple nodes over a period of time with maximum throughput. The accuracy value is determined by comparing the intended value of counter over a period of time. e.g. counter = 1000 and if the accuracy is ± 0.1%. This means the actual value of counter observed is between 990 and 1010. We observed that the accuracy index deviates between ± 0.16% as the number of nodes increases.

In summary, we were able to benchmark the performance of the SLA Enforcement prototype over InfiniBand and Ethernet. The observation clearly proves that InfiniBand out performs Ethernet by a factor of 8. Secondly, since performance was not the only quality presented at the requirement phase, we exercised the prototype over InfiniBand and Ethernet and recorded the CPU usage. As a result we proved that the prototype uses 3 times less CPU computation when deployed over InfiniBand. Finally, we assessed the prototype to check the data integrity of the distributed SLA counters. We report a deviation of ± 0.16% that lies within the ±5% that normally required for such systems.

5. CONCLUSION AND FUTURE WORK

The study highlighted the motivation behind the rationale for Telecommunication operator to ensure a reliable and robust SLA enforcement solution across a distributed architecture for real time messaging gateways. The paper described the reasons for paradigm shift from monolithic to distributed telecommunication solutions. As a result of which the complexity of designing distributed messaging solution to address the problem of fast yet reliable inter node conversation has increased. Consequently, the investigation resulted to the proposition of a novel clustering method.

The paper described our work on deploying a distributed SLA Enforcement solution using InfiniBand over RDMA channel interface. We situated the problem domain in the telecommunication arena wherein, performance, data integrity and reliability are critical the quality of service. The observations from the models, (simulation and prototype) of the SLA Enforcement problem prove that the performance of the system over InfiniBand was greater than Ethernet by a factor 8. With such hyper drive, we are able to compromise some of the performance to boost data integrity. We defined Data integrity to be the correctness of the SLA counters over the distributed servers. As a result data integrity lies at ± 0.1%, well below the required value. An important aspect of the study shows that, with advanced clustering techniques using InfiniBand over RDMA concepts, the distributed servers act as if they are one single entity, although the application is expected to scale very well, further testing for scalability will carried out in future work.

REFERENCES

[1] Debusmann Markus, Keller Alexander, “SLA-driven Management of Distributed Systems using the Common Information Model”, *University of Applied Sciences*, Kurt-Schumacher-Ring 18, IBM Research Division.

[2] William T Futral, “InfiniBand Architecture, Development and Deployment; A Strategic Guide to Server I/O Solutions”, Intel Press, January 2002.

[3] G. Pfister, “An Introduction to the InfiniBand Architecture”, High Performance Mass Storage and Parallel I/O, IEEE Press, 2001.

[4] Verari Systems, www.Verari.com

[5] NSF, DARPA, MPI-2: Extensions to Message Passing Interface, November 2003.
[6] Shipman G. M., Woodall T. S., Graham R. L., Maccabe A. B., InfiniBand Scalability in Open MPI, *Master Thesis*, University of New Mexico, December 2005.
[7] Gupta R., Balaji P., Panda D. K., and Nieplocha J., Efficient Collective Operations using Remote Memory Operations on VIA-Based Clusters, in *International Parallel and Distributed Processing Symposium (IPDPS '03)*, April 2003.
[8] Magoutis K., Addetia S., Fedorova A., Seltzer M., Chase J., Gallatin A., Kisley R., Wickremesinghe R., and Gabber E., Structure and performance of the direct access file system, in *Proceedings of USENIX 2002 Annual Technical Conference*, Monterey, CA, June 2002.
[9] Buyya R, GridBus: A Economy-based Grid ResourceBroker, University of Melbourne, 2004.
[10] Cluster Resources, Maui Scheduler Administrator Guide, version 3.2, 2005.
[11] In Jang-uk, Avery P., Cavanaugh R., and Ranka S., Policy Based Scheduling for Simple Quality of Service in Grid Computing, in *International Parallel & Distributed Processing Symposium (IPDPS)*, Santa Fe, New Mexico April 2004.

Dr Souheil Khaddaj is a Reader and is leading the Component & Distributed Systems Research Group (CODIS) at Kingston University. He completed his PhD in Computer Science at Queen Mary and Westfield College, University of London. He has been active in research and development using novel computer architectures and technologies for numerous applications since 1990. His research interests cover diverse environments ranging from scalable high performance clusters to mobile computing devices with dynamic interaction of computing and information resources. He has been involved in a number of national and international research projects and has authored/co-authored over 60 technical papers.

Bippin Makoond holds a BSc (Hons) in Software Engineering. At present, he is reading for a PhD in modelling and simulation of multi agent systems for wireless networks at Kingston University. He has worked as Lead Researcher for a software house and is the inventor of 3 patented works in the area of wireless telecommunications. He is a Consultant and Research Scientist with a specific focus on the development of Systonomy's advanced tools and techniques and the integration of software simulation engines to the Six Sigma process. He also works with software organisations to help reduce the cycle time associated with generating high technology intellectual property.

David CC Ong has more than six years industrial experience in the fields of web-based services, application development, database design and mobile messaging services. He has worked as researcher and developer in the telecommunication industry specialising in the design of mobile messaging infrastructure for the mobile phone operators. Currently he works as a researcher at Kingston University under a joint research programme with one of the University's industrial partners. He has been a member of the British Computer Society (MBCS) since 2003. He holds a BSc (Hons) in Computer Science and an MSc in Data Communications. At present, he is reading for a PhD in Computer Science at Kingston University, London.

Dr Radouane Oudrhiri is a CTO of Systonomy. He has more than 18 years of teaching, research and consulting in software engineering, architecture, process and quality improvement methods and strategies, including Six Sigma, DFSS and SW-CMM. He acts as a Strategic Consultant and Architecture Authority. Radouane has wide experience of heterogeneous and Distributed Architectures, architecture standards, styles and methods. Radouane has an M.S. in Operations Research from ENSAE Paris, an MBA from ESSEC Paris and a Ph.D. in Information Systems andTheory from ESSEC and Universite d'Aix-Marseille. He is also a lecturer in software engineering at the French Engineering Telecommunication School.

A Multicast Administration Method in FTTH*

Li Wang [1] Xuexian Cheng [2] Chuanqing Cheng [3]
[1]School of Telecommunication,Wuhan University
[2]Hubei University of Technology
[3]Wuhan University of Science and Engineering
Wuhan,China
Email: [1]wl3833@126.com

ABSTRACT

With the internet development and popularization, the demand of service gets a rapid growth. As the trunk network is tending toward perfection, the bandwidth of access network is becoming the bottleneck of service needs. Ethernet Passive Optic Network (EPON) is a new technology which is considered one of the best solutions of access network. It is the best way to achieve FTTH. This paper discussed the multicast administration method in FTTH device. The paper points out the multicast control and administrator have been imported to FTTH, discussed some controllable multicast parameter. Finally a multicast administration method of EPON is presented.

Keywords: EPON IGMP Proxy IGMP Snooping Multicast

1. INTORDUCTION

With the rapid development of optical network, the EPON network based on fiber communication technology have started an application. EPON breaks the bandwidth of ordinary transmission line and can transmit multiple services, such as IPTV/DATA/VOICE. It is a novel optical access network technology, deploying point to multi-points structure, passive transmission on fiber, supplying service on Ethernet. It adopts PON technique on physical layer and Ethernet technique on data link layer and implements Ethernet access with PON structure. The services of multicast have the common character of that the single source information can be received by multi end station.

However there are some shortcomings of the development of multicast service. The key disadvantage is that the multicast related protocol ignores the controllable and manageable demand from service-supplier, because of the history reason that the design of multicast protocol is designed based on LAN. But controllable and administrable device is essential to device-supplier. So the controllable-multicast has recently attracted more and more attentions since it ban be a perfect solution to the multicast service-supplier.

The section 2 introduced multicast control and administration, include project demand, background, bring forward some parameter of controllable multicast. Section 3 discribed a detailed controllable multicast scheme in EPON system .Section 4 is conclusion and future work.

2. BACKGROUND

EPON system is device with high port consistency and high reliability. The main structure of EPON is as Fig.1:

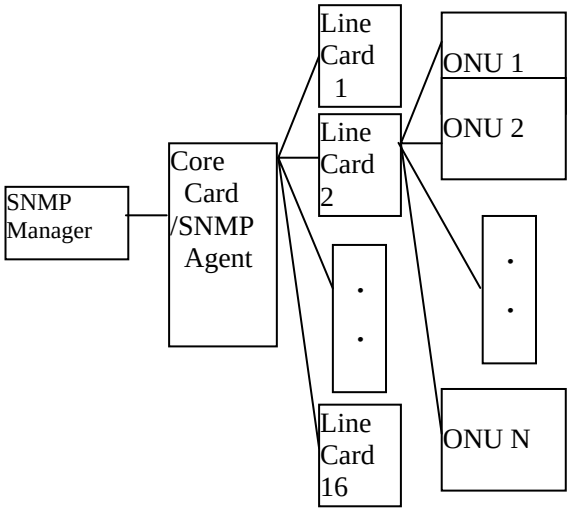


Fig.1. EPON System Structure

In EPON system, there are three downstream communication ways: unicast, multicast, broadcast. When the network running in multicast way, the packet from OLT can only be received by onus which is set in advance, other onu will not process the information. OLT only need to send a multicast stream, which can not only decrease the waste of bandwidth and improve the using rate of downstream bandwidth, but also distribute the pressure of EPON.

EPON deploys broadcast way in downstream direction. The downstream data broadcast to all of the onus. Each onu filter packets and receive own one. Both RS layer and MAC layaer can filter multicast packets. The difference is like following:

2.1 MAC Filtering

If multicast filter is on MAC layer, the broadcast LLID can be used. (1) Use Default LLID for all traffics with multicast MAC address (2) MAC Layer discard frames with unknown multicast MAC address. (3) RS Layer does nothing about all multicast traffics. (4)RS is responsible for filtering unicast packet. MAC is responsible for filtering multicast packet.

When the onu received the packet, all the multicast and broadcast LLID can pass the RS layer. Then the unknown MAC address which has passed the RS layer will be dropped.

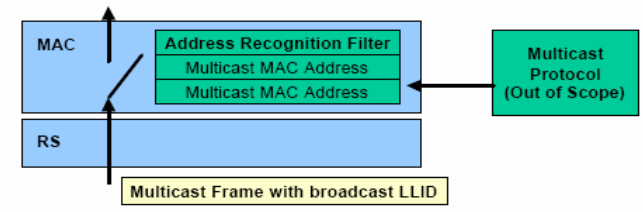


Fig.2. MAC Filtering

* This work is supported by Hubei Province Natural Science Foundation under Grant 2006ABA296.

2.2 RS Filtering

Other method is to filter multicast packet on RS layer A multicast LLID must be defined with another mode bit.,RS Layer will discard frames which has unknown multicast LLID.MAC Layer may not require another filtering for the multicast. Mapping the multicast MAC address to the multicast LLID has to be defined. The map method can be Hash function or direct mapping

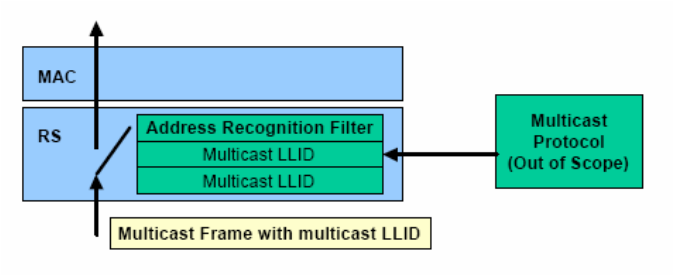


Fig.3. RS Filtering

There is an obvious shortcoming of this method because it is not compatible with. IGMP proxy or IGMP snooping protocol. The IGMP protocol family is based on the multicast MAC address (01005e******).So the MAC address filter is selected.

3. MULTICAST SHORTCOMING

IP multicast technology is very important to the novel multimedia service apply. IGMP proxy or IGMP snooping are the most widely used protocols. IGMP proxy is more enhanced than IGMP snooping. IGMP Proxy performs different function on the uplink port and downlink port, the system load is more than IGMP snooping. The best thing is that IGMP Proxy can take the task of query-station when there is no router in network. Moreover, if IGMP module to be enhanced, IGMP Proxy is more convenient than GIMP snooping since it head off the all IGMP protocol packets.

However, there are some problems of multicast service from the point of service supplier. The main problems are user management and service management.

First, there is no authentication mechanism in multicast protocol. The user may join a group or leave it freely. The multicast source (multicast service supplier) have no way to know the accurate time the user join or leave, and to stat. how many users are receiving the multicast stream at a period.

Second, multicast source (multicast service supplier)is lack of effective measures to control the direction or area of the multicast stream in the network .The multicast source play a role of "video on demand". It is the key obstacle of the multicast source supplier to supply more services.

Third, multicast protocol doesn't give assure of safty. Any user can be regarded as a multicast source to send stream. There is lack of control of multicast source. In a network supporting multicast service, there may be legal multicast sources and illegal multicast sources.

So there is an imperious demand to optimize and improve multicast function, make it can be fit for the present running network actuality

sending the specifically membership query packets when receiving a leave packet.

Presently there is no normal criterion of controllable multicast. But the framework is clear gradually. It involves user management, source management and user information record.

The following is the detail of the parameter.

- on-line group amount, the multicast address of the group, membership of the group and etc.
- preview information，which means when the host's purview is preview, it can join in a group temporally and be forced to leave when timeout.
- source management: can control the source IP range (multicast IP)which connect to the device supporting multicast.
- Authentication of host port. can configure the purview to be permit/forbidden/preview. When the host port would join a group, it must do authentication first. All the operation of the host must be limited to its purview
- log information, can show the join/leave information of host port, include port ID, the multicast address of the group ,the time of join/leave.

4. A MULTICAST ADMINISTRATION METHOD

4.1 Multicast in EPON without Control

IGMP Proxy can take the task of query-station when there is no router in network. Moreover, if IGMP module to be enhanced, IGMP Proxy is more convenient than IGMP snooping since it head off the all IGMP protocol packets .So the scheme we put out is on the basis of IGMP Proxy.

We give an ordinary IGMP Proxy model first. Fig.4 gives the flow. It is the foundation of multicast control & administration.

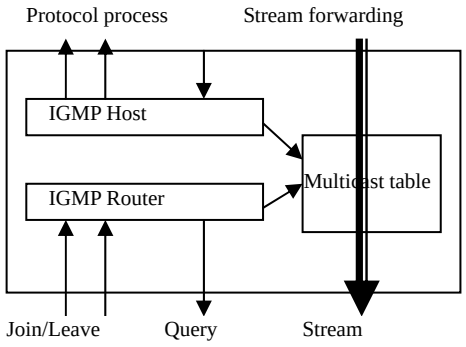


Fig.4. Ordinary IGMP Proxy Model

4.2 Multicast in EPON with Control

On the basis of the ordinary module，importing the parameter we introduced in section 3，we give a controllable multicast scheme as the Fig.5

Network management module configure the control information of multicast, multicast control module will form some access table, such as multicast source table, user table, user purview table and etc. When IGMP Proxy module process the protocol packet, it must check the access table first, and change some ordinary action. In this scheme, the multicast

table's form is not only by protocol packets but also by the control module. If a host port is not forbidden to access the source, or the source is not legal. (which is configured by network management module),then the join packet in which the host port want to join the source will be ignored.

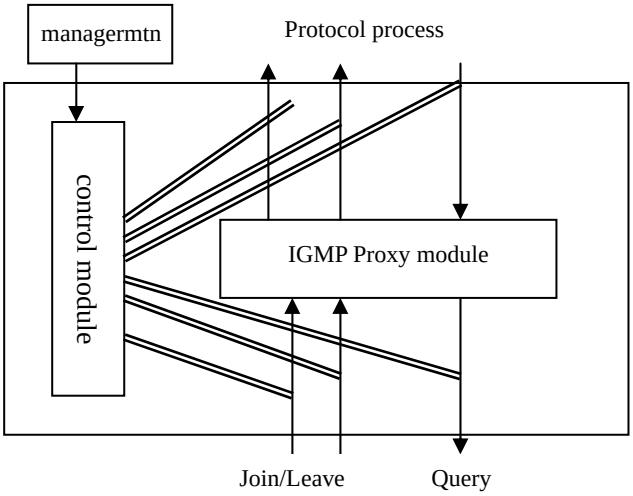


Fig.5. Controllable Multicast

4.3 Onu Join the Multicast Group

When the STB (set-top box) of an onu hope to join the multicast group, it will send a join packet to device. Onu receive the IGMP join packet, if the host should join a new group, onu will send the join packet to OLT. OLT will check the administration table to check if the user has rights to get multicast stream. If yes ,it will forward it to notify router and add this port to the multicast table .If the group have been exist, only add this port ,and startup the timer of this port. Else if the port has been the membership, only flush the timer. If no, the join packet will be dropped. The timer is running. If the user's right is preview, when the timer expires, the port will be forced to leave the group and can not received the multicast stream any longer. All information will be recorded in the step, such as which port, when ,join which group., what is the time of start, what is the user's right, preview. deny or permission? All of the information formed log to be viewed by manager.

4.4 Onu Leave the Multicast Group

When the STB (set-top box) of an onu want to leave the multicast group, it will send a leave packet to onu. When receive leave packet, the onu will send the packet to OLT. OLT send specifically query packet to the user. If not received the membership report packet after three query, then delete this port from the group. If the group have no member,Delete the group and send a leave packet to notify router. Under administration, the leave time will be recorded.

4.5 Membership Query Packets

When the query packets received from multicast router, OLT is responsible for reporting the current group to the router.

The upper scheme maintains a multicast table, the stream forward accruing to the table. From the flow, we know there is no control to multicast stream. As long as IGMP protocol packets received in the device, multicast table will form, the stream will forward.

5. CONCULUSIONS

In this paper, we analysis the background of multicast control and administration, The paper points out the multicast control and administrator have been imported to FTTH, discussed some controllable multicast parameter. Finally a multicast administration method of EPON is presented.

REFERENCES

[1] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Translated J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digest 9th Annual Conf. Magnetics Japan, p. 301, 1982]. M. Young, The Technical Writer's Handbook, Mill Valley, CA: University Science, 1989.

[2] Parkhurst WR. Cisco Multicast Routing And Switching. McGraw Hill, 1999, pp.25~42, pp.43~53.

[3] Deering S. Host extensions for IP multicasting. RFC 1112, Stanford University, 1989.

[4] Fenner W. Internet group management protocol. Version 2, RFC 2236, Xerox PARC, 1997.

[5] Cheng Chuanqing, Wang Li IP multicast group management protocol and implementation in L2 *information technology*，Sep 2003.

[6] Biswas S, Haberman B, Cain B. IGMP multicast router discovery. Nortel Networks and Cereva Networks. Internet-Draft, 2001.

[7] B.Cainetal，Internet，Group Managem ent Protocol，Version 3, RFC3376,Oct 2002.

[8] Fenner B, He HX, Haberman B, Sandick H. IGMP-Based multicast forwarding (IGMP proxying). AT&T-Research, Nortel.

[9] IEEE P802.3ah task force.IEEE Draft P802.3ahTM/D1.9, Operations,Administration and Maintenance(OAM). http://www.ieee802.org/3/efm,2003-02-31.

A New QoS Multicast Routing Algorithm Using Ant Algorithm*

Bencan Gong, Layuan Li
Department of Computer Science and Technology, Wuhan University of Technology
Wuhan, 430063, P. R. China
Email: [1]gonbc@tom.com

ABSTRACT

QoS Multicast routing has been a very important research issue in the areas of network and distributed system. In this paper, we propose a new QoS multicast routing algorithm (NQMRA). The traditional ant algorithm is improved to be suitable for QoS routing problem. Firstly the crossover operation of genetic algorithm is used to optimize the solution and quicken the convergence. In addition, we modify the state transition rule and pheromone updating rule of ant algorithm to effectively guide ants' movement and ensure the feasibility of a solution. Simulation results show that NQMRA can find the optimal or sub-optimal solution quickly and is a feasible approach to QoS multicast routing.

Keywords: QoS, Multicast Routing, Ant Algorithm, State Transition Rule, Pheromone Updating Rule

1. INTRODUCTION

QoS multicast routing has attracted much interest with the emergence of group-based real-time applications that require strict quality of service (QoS), e.g., video conferencing, remote education, and distributed multimedia service. For group communication, multicast is more efficient than unicast, because sender only transmits a copy of data to a group of receivers instead of sending separate copy to each receiver. However, the realization of QoS multicast routing is very difficult. Finding a feasible route with two independent QoS constraints is NP-complete [1]. The traditional multicast routing protocols [1-4] are designed for best-effort data delivering, which can not satisfy QoS requirements when network resources are scarce.

Some algorithms [5-8], e.g., BSMA [6], KPP [7], provide heuristic solutions to the constrained Steiner tree problem, which can find the delay-constrained least-cost multicast tree. BSMA is based on a search optimization way, which first creates a least-delay tree, and then iteratively improves it by removing high-cost paths from the tree. KPP applies Prim's algorithm to construct a Steiner tree in a complete graph. These algorithms are not suitable for Internet environment because they require global network information and have excessive computation overhead.

An alternative is to use artificial intelligence (AI) approaches such as genetic algorithm [9-10], ant algorithm [11-14] and so on. Ant algorithm performs well in solving the Traveling Salesman Problem (TSP). Many characteristics of TSP are similar to those of QoS multicast routing. Therefore, ant algorithm is a viable approach for solving the problem. The essential characteristics of ant algorithm include positive feedback, distributed computation and greedy heuristic search, which help to solve the NP-hard problem.
This paper is organized as follows. Section 2 presents the network model of QoS multicast routing. Section 3 describes the key ideas of algorithm. Section 4 introduces the implement procedure. Section 5 is the discussion. Section 6 gives the experiment results. Section 7 draws a conclusion.

2. NETWORK MODEL

A network can be denoted as a weighted digraph $G = (V, E)$ where V is the set of nodes and E is the set of edges. Only those digraphs are considered in which there is at most one edge between a pair of ordered nodes. Parameters associated with each edge represent the current state of the edge.

Suppose $T(s, M)$ denotes a multicast tree, $s \in V$ is the source node of the multicast tree, $M \in \{V-\{s\}\}$ is a set of destination nodes, $p(s, t) \in T(s, M)$ is a path connecting s to $t \in M$. For simplicity, we only consider edges' QoS constraints and assume that all nodes have enough resources.

Definition 1: For any edge $e \in E$, we define: Delay function $delay(e)$, cost function $cost(e)$, bandwidth function $bandwidth(e)$, and delay jitter function $jitter(e)$. For $T(s, M)$, there are the following relations:

$$(1)\ \mathrm{delay}(p(s,t)) = \sum_{e \in p(s,t)} \mathrm{delay}(e)$$

$$(2)\ \mathrm{bandwidth}(p(s,t)) = \min\{bandwidth(e), e \in p(s,t)\}$$

$$(3)\ \mathrm{jitter}(p(s,t)) = \sum_{e \in p(s,t)} \mathrm{jitter}(e)$$

$$(4)\ \mathrm{cost}(p(s,t)) = \sum_{e \in p(s,t)} \mathrm{cost}(e)$$

$$(5)\ \mathrm{delay}(T(s,M)) = \max\{delay(p(s,t)), p(s,t) \in T(s,M)\}$$

$$(6)\ \mathrm{bandwidth}(T(s,M)) = \min\{bandwidth(e), e \in T(s,M)\}$$

$$(7)\ \mathrm{jitter}(T(s,M)) = \max\{jitter(p(s,t)), p(s,t) \in T(s,M)\}$$

$$(8)\ \mathrm{cost}(T(s,M)) = \sum_{e \in T(s,M)} \mathrm{cost}(e)$$

Definition 2: Assume that delay constraint of multicast tree is DL, bandwidth constraint is BW, and delay jitter constraint is DJ. QoS multicast routing is to find a $T(s, M)$, which satisfies the following relations:

$$(1) delay(T(s,M)) \le DL$$

$$(2) bandwidth(T(s,M)) \ge BW$$

$$(3) jitter(T(s,M)) \le DJ$$

Meanwhile, $cost(T(s, M))$ should be minimal.

3. KEY IDEAS OF ALGORITHM

3.1 Data Structure

To easily realize the algorithm, we devise the data structures of ant, edge and node. They are shown in Table 1, Table 2 and Table 3.

* This work is supported by the National Natural Science Foundation of China (No. 60672137) and Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20060497015).

Table 1. Data structure of the ant

field name	Comment
tabu[]	set of nodes passed by the ant
c	cost of the path passed by the ant
dl	delay of the path passed by the ant
dj	delay jitter of the path passed by the ant

Table 2. Data structure of the node

field name	Comment
bh	number of the node
upnode	upstream node of the node
outdegree	out degree of the node
flag	flag denoting whether the node is in tree

Table 3. Data structure of the edge

field name	Comment
node1	one endpoint of the edge
node2	another endpoint of the edge
phero	pheromone of the edge
c	cost of the edge
dl	delay of the edge
dj	delay jitter of the edge
bw	bandwidth of the edge
flag	flag denoting whether the edge is in tree

3.2 State Transition Rule

For ant algorithm, its first task is to choose a neighboring node according to the amount of pheromone on edges. To satisfy QoS requirements, we modify the state transition rule of ant algorithm. The new rule is as follows:

The ant *k* positioned on node *i* chooses next node *j* to move to by applying the rule given by Eq. (1)

$$j = \begin{cases} d^k, & if\ R \\ J, & otherwise \end{cases} \qquad (1)$$

where d^k is the destination node which the ant *k* is searching, *J* is a random variable selected according to the probability distribution given in Eq. (2), *R* is the following condition expression:

$$\exists e(i,d^k) \wedge bw(i,d^k) \geq BW \wedge delay(p^k(s,i)) + dl(i,d^k) \leq DL$$
$$\wedge\ jitter(p^k(s,i)) + dj(i,d^k) \leq DJ \wedge q \leq q_0$$

where $bw(i,d^k)$, $dl(i,d^k)$ and $dj(i,d^k)$ denote bandwidth, delay, and delay jitter on edge (i,d^k) respectively, $p^k(s,i)$ is the path passed by the ant *k* from the source *s* to the current node *i*, *q* is a random number uniformly distributed in [0···1], and q_0 is a constant. When a neighboring node is the destination node and satisfies QoS requirements, the ant *k* will move to the destination node with the probability q_0.

IF *R* can not be satisfied, the ant *k* chooses to move to node *j* according to the following probability:

$$P^k(i,j) = \begin{cases} \dfrac{[\tau(i,j)]^\alpha \cdot [\eta(i,j)]^\beta}{\sum_{s \in J^k(i)} [\tau(i,s)]^\alpha \cdot [\eta(i,s)]^\beta}, & if\ j \in J^k(i) \\ 0, & otherwise \end{cases} \qquad (2)$$

where α and β are two parameters which determine the relative importance of pheromone intensity versus heuristic information on edge*(i, j)*, $\tau(i,j)$ is the pheromone intensity on edge*(i, j)*, $\eta(i,j)$ is the heuristic information on edge. We set $\eta(i,j) = 1/(dl(i,j) + dj(i,j))$. $J^k(i)$ denotes a set of nodes that satisfy the following condition:

$$\exists e(i,j) \wedge bw(i,j) \geq BW \wedge delay(p^k(s,i)) + dl(i,j) \leq DL$$
$$\wedge\ jitter(p^k(s,i)) + dj(i,j) \leq DJ \wedge j \notin tabu^k$$

where tabu^k is the set of nodes that the ant *k* has visited.

3.3 Pheromone Updating Rule

For ant algorithm, its second task is to adjust the amount of pheromone. In NQMRA, we use the best ant strategy. After all ants have completed their paths, the level of pheromone on edges along the path visited by the best ant is updated by applying the following pheromone updating rule:

$$\tau(i,j) = \rho \cdot \tau(i,j) + \Delta\tau(i,j)$$

$$\begin{cases} \Delta\tau(i,j) = \dfrac{Q}{\cos t(p(s,t))}, & if \quad e(i,j) \in p(s,t) \\ \Delta\tau(i,j) = 0, & otherwise \end{cases} \qquad (3)$$

where ρ (0< ρ <1) is pheromone decay parameter, Q is a constant, *p(s,t)* denotes the path by the best ant from the source *s* to destination node *t*, $\Delta\tau(i,j)$ is the pheromone amount left on edge*(i,j)* by the best ant.

How to judge which ant is the best ant? The traditional method is that the ant whose path is shortest among all paths is the best ant. But the method is not suitable for the multicast routing problem. In our algorithm, the best ant can be described as:

$$\arg \quad \min_{1 \leq k \leq m} \{ \sum_{e \in R} \cos t(e), R = p^k(s,t) - T(s,M) \}$$

where *m* is the number of ants, the path and the multicast tree are represented as the set of edges. We take an example in Fig.1 to illuminate the idea.

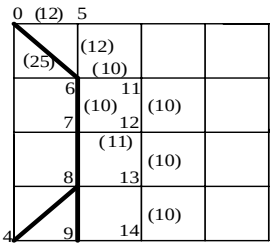


Fig.1. An example illuminating the best ant

In Fig.1, the number of nodes and the cost of edges have been labeled, and the bold lines denote the multicast tree. Node 0 is the source, and 4,9,14 are the destination nodes. Our approach of constructing a multicast tree is to find the shortest paths from the source to each destination separately by ant algorithm and then merge the resulting paths to form a tree. The two paths from 0 to 4 and from 0 to 9 have been added into the multicast tree. When ants search the destination 14, the path by an ant is (0,5,6,11,12,13,14), and the path by another one is (0,6,7,12,13,14). The former cost is 64, and the later cost is 66. However, the later ant is the best ant. Because the cost increment of the multicast tree, i.e. the cost sum of three edges (7-12, 12-13 and 13-14), is only 31 when the later path joins the multicast tree, and far less than former increment 64.

3.4 Crossover Operation

In the algorithm, crossover operation belonging to genetic algorithm is used to explore new paths and hopefully find better paths. In order to perform crossover operation, two shorter paths are selected from all paths visited by ants. To ensure that the generated paths are still valid, the two paths must have at least one common node except the source and destination node. If there are many common nodes, one of them

will be randomly selected. The chosen node is called crossover point. Crossover operation will exchange the first portion of path 1 with the second portion of path 2 and vice versa.

It is possible that loops occur after crossover operation is executed. Loops can be eliminated by searching the repeated nodes along the path and deleting the nodes between the repeated nodes. If the results are better, the new paths will replace the old paths.

4. IMPLEMENT PROCEDURE

Firstly we give some explanations and assumptions as follows. Let that there are *W* destinations, *W* types of ants, *W* types of pheromones, and every type of ants consists of *m* ants. We use one type of ants to search one destination correspondingly, and assume that the properties of pheromone deposited by different type of ants are different from one another. *T_E* and *T_N* denote the set of edges and the set of nodes in the multicast tree respectively.

The steps of the proposed algorithm are given as follows:

Step1: Initialize network nodes.
Set *NC:* = 1; (*NC* denotes a loop counter)
Initialize every type of pheromone amount on edges;
Assign initial value to *(dl, dj, bw, c)* for every edge and the constraints *(DL, DJ, BW)*;

Step2: Initialize multicast tree.
$T\_E = \phi$;
$T\_N = \phi$;

Step3: From the source node, search a destination node and add it into the multicast tree.
Choose a node $d\ (r) \in M$ randomly with equal probability;
Put the *r-th* type of *m* ants to the source node *s*;
Every ant puts *s* into tabu table, and chooses next node *j* by Eq. (1)(2);
If no node satisfies QoS requirements, the ant will empty tabu table, go back to the source node and search again;
Else the ant moves to *j,* puts *j* into tabu table; calculate *c, dl* and *dj* of the ant *k* as the following equation:

$$ant^k.c+ = c(i, j)$$
$$ant^k.dl+ = dl(i, j)$$
$$ant^k.dj+ = dj(i, j)$$

Ants repeat the choice process until all of them reach *d(r);*
Perform crossover operation;
Select the best path;
Update pheromone amount by Eq. (3);

Step4: check whether all destination nodes have been found.
$M=M-\{d(r)\}$;
If $(M \neq \phi)$ then goto step3;

Step5: merge the best paths from the source to each destination to form a multicast tree.
Suppose that there is a path (s, t_1, t_2, ···, d_1) to join. From the destination node d_1, examine every node along the path;
If $t_i \notin T\_N$, add node t_i and the corresponding edge (t_i, t_{i+1}) into *T_N* and *T_E* respectively;
$t_{i+1}.upnode = t_i$;
$t_i.out\deg ree++$;
Else if in the multicast tree, the path for *s* to d_1 satisfies QoS requirements, then join process ends; else prune a branch toward the upstream of the multicast tree until the current node $n \in T\_N \,||\, n.out\deg ree > 0$, and then continue the join process from the node t_i.
Compute cost, delay and delay jitter of the multicast tree, and save the best result up to now;

Step6: check stop condition.
If $(NC \leqslant NC_{max})$
Then empty tabu table and goto step2;
Else print the minimum-cost multicast tree;

5. DISCUSSION

5.1 Correctness proof

Theorem 1: The multicast tree found by NQMRA is Loop-free.

Proof: Each ant has tabu table that records the visited nodes, and each node has a unique identifier, thus ants do not make loop. In crossover operation, the results are examined to ensure loop-free by searching the repeated nodes along paths and deleting nodes between the repeated nodes. In addition, when the best paths join the multicast tree, the pruning operation can avoid creating loop; therefore, the generated multicast tree is loop-free. The theorem holds.

Theorem 2: The multicast tree found by NQMRA is the optimal or sub-optimal tree that satisfies QoS requirements.

Proof: As mentioned before, the ant at current node *i* will select next node *j* according to the following condition:

$$(bw(i, j) \geq BW) \wedge (delay(p(s, i)) + dl(i, j) \leq DL) \wedge (jitter(p(s, i)) + dj(i, j) \leq DJ)$$

Thus all paths by ants satisfy QoS requirements. In the merging process, the pruning operation ensures the joining path to reach QoS requirements. In addition, the paths used by NQMRA are the minimum-cost paths; therefore, the constructed multicast tree is optimal or sub-optimal. The theorem holds.

5.2 Ant Number

It is very difficult to determine the needed ant number because more ant number can accelerate the convergence of algorithm, but will increase the overhead of network. Our algorithm ensures that the every path by ants is feasible and avoids a large number of useless solutions; therefore, we can set less ant number. According to the results of extensive simulation experiments, we set ant number m=|V|/5 where |V| denotes the number of network nodes. However, many ant algorithms make the needed ant number equal the number of nodes in network.

6. SIMULATION EXPERIMENTS

The proposed algorithm is implemented and a series of simulation experiments are conducted to test the correctness and performance of NQMRA. The experiments are conducted using a 5×5 mesh network depicted in Fig.2. The parameters are set as following: $\alpha = 1$, $\beta = 2$, $\rho = 0.8$, $m=5$, $W=5$, $NC=10$, $q_0=0.6$. The characteristics of edge can be described by a fourtuple *(dl, dj, bw, c)* where *dl, dj, bw, c* denote delay, delay jitter, bandwidth and cost respectively. The source node is 0 and the set of destination nodes is {4, 9, 14, 19, 24}.

Suppose delay constraint *DL=20*, delay jitter constraint *DJ=30* and bandwidth constraint *BW=40*, the generated multicast tree is shown in fig.3 (a). Cost, delay and delay jitter of the tree are

129, 20 and 30 respectively.

Suppose *DL=30, DJ=40* and *BW=40*, the generated multicast tree is shown in fig.3 (b). Cost, delay and delay jitter of the tree are 122, 26 and 39 respectively. The convergence curves of NQMRA are in Fig.4. The figure shows the cost curve of NQMRA declines continuously, the optimal solution can be found quickly, and the curves of delay and delay jitter vibrate slightly.

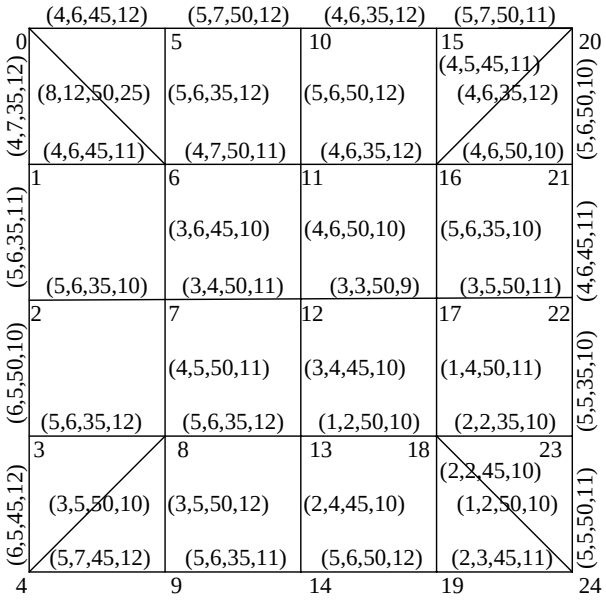


Fig.2. An example network graph

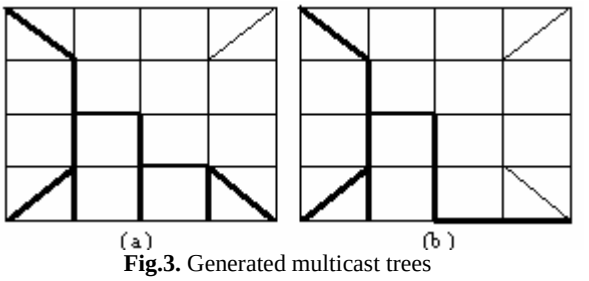


Fig.3. Generated multicast trees

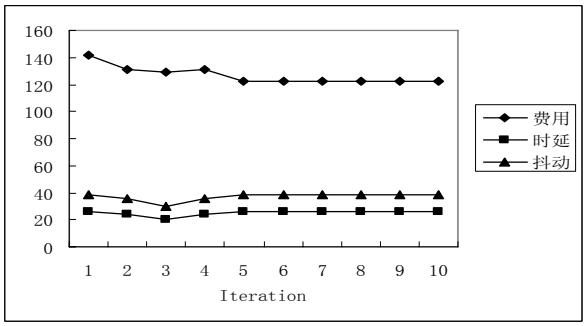


Fig.4. Convergence curves of NQMRA

7. CONCLUSIONS

We present a new QoS multicast routing algorithm based on ant algorithm. The algorithm has the following characteristics: (1) NQMRA considers multiple QoS metrics to construct a minimum-cost multicast tree. (2)NQMRA can find the optimal or sub-optimal solution quickly and has good performance. (3) In NQMRA, each node forwards ants only to one neighboring node instead of all near nodes, and no routing table is exchanged between nodes, therefore, compared with flooding, it has very small overhead.

REFERENCES

[1] K.Carberg and J.Crowcroft, "Building shared trees using a one-to-many joining mechanism." *ACM Computer Communication Review*, Jan.1997, pp.5-11.

[2] T.Ballardie, P.Francis and J.Crowcroft, "An architecture for scalable inter-domain multicast routing." in *Proc of ACM SIGCOMM 93, San Francisco*, CA. Oct 1993, pp 85-95.

[3] Li Layuan, "A new formal specification technique for communication protocol," In *proc. IEEE INFOCOM*, 1989, pp.74-81.

[4] L. Kou, G. Markowsky, and L. Berman, "A Fast Algorithm for Steiner Trees," *Acta Informatica*, 15, pp.141-145, 1981.

[5] Li Layuan, Li Chunlin, "A distributed multicast routing protocol with QoS constraints," *Networks, ICON 2002 10th IEEE International Conference on* 27-30 Aug 2002 pp.37-42.

[6] Qing Zhu, Parsa, M., Garcia-Luna-Aceves J. J., "A source-based algorithm for delay-constrained minimum-cost multicasting," proc. *IEEE INFOCOM* 95, boston, MA, Apr 1995.

[7] V. P. Kompella, J. C. Pasquale, and G. C. Polyzos, "Multicasting for multimedia applications," in *Proc. IEEE INFOCOM'92*, 1992, pp. 2078–2085.

[8] Q. Sun and H. Langendoerfer, "Efficient multicast routing for delay sensitive applications," in *Proc. Second Workshop Protocols Multimedia Systems* (PROMS'95), Oct 1995, pp 452–458.

[9] Li Layuan, Li Chunlin, "QoS multicast routing algorithm based on GA," *Journal of Systems Engineering and Electronics*, Vol.15, No.1, 2004, pp 90-97.

[10] Yussof, S., Ong Hang See, "QoS Routing for Multiple Additive QoS Parameters using Genetic Algorithm," *Networks, Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication, 2005 13th IEEE International Conference on Volume* 1,16-18 Nov. 2005, pp.99-104.

[11] M. Dorigo, L. M., Gambardella, Ant colony system: "A cooperative learning approach to the traveling salesman problem." *IEEE Transactions on Evolutionary Computation,* 1(1997), pp 53-66.

[12] Ziqiang Wang, Dexian Zhang, "A QoS multicast routing algorithm based on ant colony algorithm." *Wireless Communications, Networking and Mobile Computing, 2005 International Conference on* Volume 2, 23-26 Sep 2005, pp.1007 –1009.

[13] G.Lu, Z.Liu and Z.Zhou, "Multicast Routing Based on Ant Algorithm for Delay-Bounded and Load-Balancing Traffic," *25th Annual IEEE Conference on Load Computer Networks,* pp.362-368, 2000.

[14] Y.Wang, J.Xie, "Ant Colony Optimization for Multicast Routing," *The 2000 IEEE Asia-Pacific Conference on Circuits and Systems,* pp.54-57, 2000.

Bencan Gong was born in 1970. He is currently Ph. D. candidate in Computer Science and Technology of Wuhan University of Technology. His research interests include QoS multicast routing, distributed computing, network optimization, ad hoc networks and protocol engineering. He has published

over 10 technical papers.

Layuan Li was born in Hubei in 1946. He is currently a professor and Ph.D. tutor of computer science, and editor in Chief of the Journal of WUT. He is director of International Society of High-Tech. and paper reviewer of IEEE INFOCOM, ICCC and ISRSDC. His research interests include high-speed computer networks, protocol engineering and image processing. He has published over one hundred and fifty technical papers and is also the author of six books. He was awarded the National Special Prize by the Chinese government in 1993.

The Reverse Path Join Multicast Protocol based on the Probability *

Hui Lü, Yanxiang He, Dandan Yu
School of Computer,Wuhan University
Wuhan, Hubei, 430072,China
Email: lvhui_ta@tom.com

ABSTRACT

This paper proposes the Reverse Path Join Multicast protocol based on the probability(RPJMPP).The RPJMPP will discover some paths which can't easily reach the target sender. The probe message won't be forwarded from the discovered paths. So the flooding is avoided. Using analysis, the complexity of RPJMPP is O(n) and the number of probes in the RPJMPP is at most the number of probe messages in the directed reverse path join (DRPJ)protocol. Through simulation, it is shown that the RPJMPP protocol reduces probe messages.

Keywords: Multicast, the Directed Reverse Path Join (DRPJ) Protocol, Probability

1. INTRODUCTION

Multicast is a selective one-to-many transmission mode [1,2] . Only a singe transmission is necessary for sending the same information to n receivers, while n independent transmissions would be required using one-to-one unicasting. To take full advantage of the bandwidth property, it is important to find paths that are shared by receivers. The collection of paths forms a multicast tree. In a multicast tree, the multicast sender is the root and group members are a subset of all the nodes in the network. Because multicast membership is dynamic, meaning each receiver can join and leave a multicast session at any time , multicast routing is needed to find the best path from a joining node to a multicast neighbor node [3,4,5] . The neighbor node is currently a part of the multicast tree for the requested multicast session. Each receiver initiates the neighbor search to find the path whenever it wants to join a multicast session .For searching a path, a joining node sends a probe message. The intermediate nodes forward all new probe message and discard previously forwarded probe messages. So the probe message will produce more probe messages. These probe messages will traverse the network and record the paths.

One of the most significant problem in current multicast protocols is the large messaging overhead to find the best multicast neighbor. The high messaging overhead becomes an especially serious problem if multicast membership changes dynamically. In this paper, a new strategy is proposed to reduce overhead.

The remainder of this paper is organized as follows. In Section 2,existing work in multicast routing is reviewed focusing on the Flooding with TTL[6] and the directed reverse path join(DRPJ) protocol[7].In section 3, the new protocol is described .Section 4 contains a simulation comparision. Section 5 is a conclusion.

2. THE FLOODING WITH TTL AND THE DRPJ PROTOCOL

* Supported by National Natural Science Foundation of China(90104005).

2.1 The Flooding with TTL

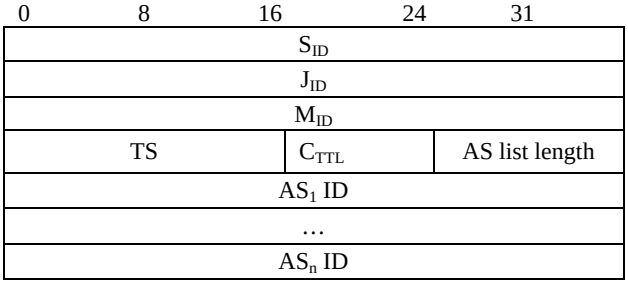


Fig.1. The probe message

The flooding with TTL is the basic protocol and finds paths by flooding the probe message. It reduces the overhead by a TTL scope. The probe message is shown in Fig.1. The key fields of the probe message contain:

Sender ID(S_{ID})
Joining node ID(J_{ID})
Multicast session ID(M_{ID})
Timestamp(TS)
C_{TTL}

S_{ID},J_{ID} and M_{ID} can be IP addresses. They respectively specify a sender, a joining node and a multicast session. Multicast group membership is specified by a combination of the sender ID and the multicast session ID. Timestamp is a unique sequence number which distinguishs the current join request from previous requests. According to the timestamp in probe messages, the intermediate node will discard the previously forwared probe messages. As a probe message traverses a network, it records each autonomous system (AS) on its path. If a matching (S_{ID}, M_{ID}) pair is found in the local routing table, the intermediate node is a multicast neighbor node of the requested multicast group. When a probe message reaches one of the multicast neighbor nodes, flooding of the probe message is stopped and the list of the propagated intermediate nodes is returned directly to the joining node. From this reply message,the joining node determines the path to one of the multicast neighbor nodes.

The flooding with TTL protocol adds the TTL field (C_{TTL}) to limit the flooding area. The TTL field is set to some threshold value(usually the hop-count distance from the joining node to the sender is used) before the probe message is flooded . On each hop, the TTL field is decreased by one.When the TTL field reaches zero,the probe message is dropped.

By the flooding with TTL protocol, multiple paths from the joining node to neighbor nodes will be found . The joining node selects one of the shortest path or the earliest returned path from some reply messages.

2.2 The DRPJ Protocol

The goal of the DRPJ protocol is to have the capability for multiple path search without blindly flooding probe messages. The DRPJ protocol introduces the concept of Maximum Deviation in hop count(D_{MD}).The D_{MD} specifies the maximum

tolerable extra path length beyond the shortest path . The D_{MD} field conveys a joining node's end-to-end delay requirement to all intermediate nodes receiving the probe message. If D_{MD}=K,all paths longer than the shortest paths up to K hops will be searched .Before the probe message is flooded from the joining node , the C_{TTL} field is set as C_{TTL} = Dj+D_{MD} where Dj is the shortest distance from the joining node to the sender.

The information included in the probe message for the DRPJ protocol is the same as the Flooding with TTL protocol. Suppose that the shortest distance to every other node is known at each node in a network. Pseudocode for the DRPJ protocol is shown in Fig.2.

```
1.  Receive a new probe message P
2.  if  (i is a part of the multicast tree for the sender)  then
3.    /* a :the address field of the probe message
      i_ID :the ID of the node i
      D_i is the shortest distance between node i and the sender*/
4.    R.a=P.a+i_ID and R.b=D_i
5.    Send a reply message R back tothe joining node
6.  else
7.    P.C_TTL=P.C_TTL-1
8.    if (P.C_TTL>D_i) then
9.      P.a=P.a+i_ID
10.   Send P from all outgoing ports except for the one P was received
11.   end-if
12. end-if
```

Fig.2. The DRPJ protocol at an intermediate node i

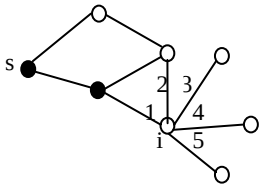
If there is a matching (S_{ID},M_{ID}) pair,a reply message is returned to the joining node by the intermediate node.If there exists no matching (S_{ID}, M_{ID}) pair , the procedure (line7,8, 9, 10,11 in Fig3) is performed.The comparision between C_{TTL} and Di ensures that a probe message will propagate further only if it is within a maximum deviation from the shortest path specified by the joining node.

3. THE REVERSE PATH JOIN MULTICAST PROTOCOL BASED ON THE PROBABILITY(RPJMPP)

The DRPJ protocol will produce a lot of probe messages(line10 in Fig2) if an intermediate node isn't the neighbor node.The RPJMPP attempts to select a subset from all outgoing ports to forward the probe message.

3.1 The Basic Principle of the RPJMPP

The probe message is to find a path between the joining node and the target sender. These paths in these probe messages don't reach the requested neighbor node.When a port receives a large number of probe messages for the same multicast group , succedent probe message for the same multicast group is possibly far away from the sender if they are forwarded from the port.



s :the sender of multicast session *m*

● :a neighbor node for the target *s* and *m*

○ :a non-neighbor node for the target *s* and *m*

numbers:the port number of the node i

Fig.3. A part of network topology

For example,Fig.3 shows a part of network topology. The node i is a non-neighbor node for the sender s. Suppose that both the port3 and the port4 receives a large number of probe messages for the target s and m.And the intermediate node i records the instance.When port5 receives a probe message P for the target s and m , the node i searches the records.Then the node i forwards P through port1 and port2.P won't be forwarded through port3 and port4.However, the DRPJ protocol will forward P through port1,port2,port 3 and port 4.

3.2 Description of the RPJMPP

The RPJMPP protocol introduces the probe table and the forwarding probability function.Each intermediate node has a probe table to record instances.The forwarding probability function helps reducing the probe messages and avoids missing some paths.

The probe table is a quad-tuple < S, M, PN, N>. *s* is an S_{ID} ($s \in S$). *m* is an M_{ID} ($m \in M$). *pn* is a port number in an intermediate node ($pn \in PN$). *n* is a counter($n \in N$), which records the number of received probe messages for target *s* and *m* on the port *pn*.Part of buffers is reserved to store the probe table at every intermediate node.The probe table isn't too large.Its maximum lenghth is limited .By the queue rule,the probe table is managed and updated. Because the topology changes dynamically,the content of the probe table is periodly cleared out.

p(n) is the forwarding probability function($p(n) \in [0,1]$).It gives the forwarding probability of received probe messages for target *s* and *m* through the port *pn*.The forwarding probability function *p(n)* should be inverse proportional to the number of received probe messages according to the example in Fig.3.And it can't fall too fast at the beginning.For computing simply,the *p(n)* is definded as follows:

$$p(n)=\begin{cases}1 & n \le T \\ \dfrac{1}{n-T} & n > T\end{cases}$$

n is the number of received probe messages for target *s* and *m* from certain port on the intermediate node *i*.T is the threshold($T \in N$,N is the set of the natural number).When the number of received probe messages for target *s* and *m* is not more than T from the port *pn*,the intermediate node will absolutely forward a new probe messages for target *s* and *m* from the port *pn*(Because of $p(n)$=1).If the number of received probe messages for target *s* and *m* is more than T from the port *pn*, the intermediate node will probably forward the new probe messages for target *s* and *m* from the port *pn*.The forwarding probability is $p(n)(p(n)<1)$.

If there isn't a matching record (*s*,*m*,*pn*,*) for certain *pn*(* stands for the wildcard character),a new probe message for target *s* and *m* will be definitely forwarded from the port *pn*.That is,the forwarding probability is regarded as 1.

Initially the TTL field is set to the hop-count distance from the joining node to the sender. Pseudocode for the RPJMPP at certain intermediate node *i* is shown in Fig.4.If there is a matching (S_{ID},M_{ID}) pair,a reply message is returned to the joining node by the intermediate node . If there exists no matching (S_{ID}, M_{ID}) pair , the procedure(line6,7,8,9,10,11 in Fig4) is performed. First the C_{TTL} and the record in the probe table are updated.If the requested delay can be satisfied,the RPJMPP will compute a forwarding probability *p(n)* for every port except for the one *P* was received.Then the new probe message will be forwarding based on every port's forwarding probability except for the one *P* was received.The

primary difference of the RPJMPP is to forward *P* from the part of ports which is the subset of all outgonging ports except for the one *P* was received .By searching the probe table and computing,some ports should be avoided when the probe message is forwarded.

1. Receive a new probe message *P* from the port *pn*
2. **if** (*i* is a part of the multicast tree for the sender) **then**
3. $R.a=P.a+i_{ID}$ and $R.b=D_i$
4. Send a reply message *R* back to the joining node
5. **else**
6. $P.C_{TTL}=P.C_{TTL}-1$
7. update the probe table set n=n+1 where (s=*P.s* & m=*P.m* & pn=*pn*)
8. **if** ($P.C_{TTL}>D_i$) **then**
9. $P.a=P.a+i_{ID}$
10. Computer the forwarding probability *p(n)* and send *P* from the port based on the probability p(n)for every port except for the one *P* was received
11. **end-if**
12. **end-if**

Fig.4. RPJMPP at an intermediate node *i*

3.3 Complexity Analysis

First of all, an intermediate node is to determine whether it is a multicast neighbor of the requested multicast session when it receives a probe message.When the RPJMPP finds a matching (S_{ID}, M_{ID}) pair in the local routing table(line 2 in Fig.4) , a linear search is required which is in the order of O(n) (n is the average of multicast session active at an intermediate node at a given time)[9].All other operations require a constant time.It is similar to the DRPJ protocol.

3.4 Probe Message Overhead

When the intermediate node isn't the neighbor node, the RPJMPP forwards *P*.If the forwarding probability is equal to 1 for every port except for the one *P* was received. The RPJMPP sends *P* from all outgoing ports except for the one *P* was received.It's similar to the DRPJ protocol.If the forwarding probability is less than 1 for part of ports, probably some ports don't send *P*.So the number of the copied probe messages is less than that of the DRPJ protocol. Therefore, the number of probes in the RPJMPP is at most the number of probes in the DRPJ protocol.

4. SIMULATION

The DRPJ protocol excels the flooding with TTL[7].We program to compare the DRPJ protocol and the RPJMPP using VC++.A network topology including 100 nodes is randomly produced.10 multicast trees will be constructed.The maximum length of the probe table is 30.The threshold T is 10.The cycle of clearing is 20 seconds.DMD in the DRPJ protocol is set to zero.The result is shown in Fig.5.

In the beginning,the probe table is null and the neighbor nodes are few.The number of probes in the RPJMPP is basically equal to the number in the DRPJ protocol and rapidly increases . After a period, the probe tables are not null and some intermediate nodes become the neighbor nodes.The number of probes decreased and keeps stably.The number of probes in the RPJPMM protocol is less than the number of probes in the DRPJ protocol.

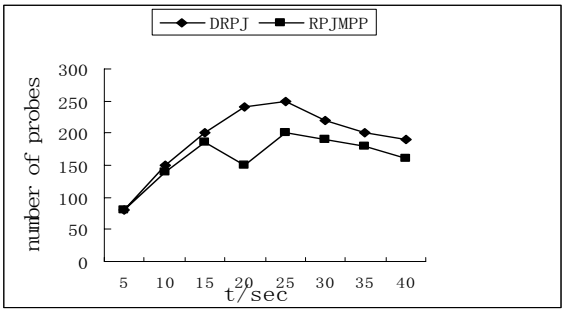


Fig.5. Comparision of number of probes

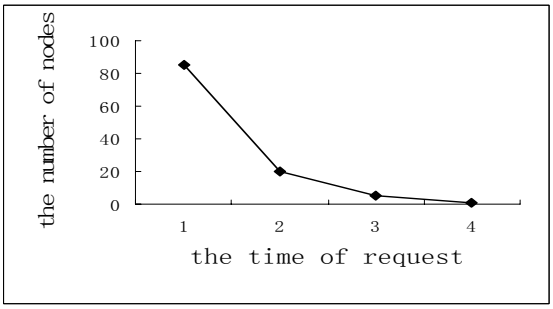


Fig.6. the time of requests for RPJMPP

The intermediate node forwards probe messages based on the probability *p(n)*.In other words, the intermediate node discards probe messages based on the probability *1-p(n)*.So it's possible that a joining node doesn't receive a reply message. If its counter expires, the joining node will repeat the joining request. The time of repeating requests is shown in Fig.6 for the RPJMPP. Fig.6 shows that the majority of the joining nodes send requests only once.

5. CONCLUSIONS

This paper proposes the new RPJMPP protocol. By the probe table, it selects a subset from all outgoing ports to forward the probe message and reduces probe messages. Evaluation shows that the complexity is equal to that of DRPJ protocol .The simulation shows that the RPJMPP helps reducing probe messages, too.

REFERENCES

[1] Jeff Doyle, Jennifer DeHaven Carroll, *CCIE Professional Development Routing TCP/IP Volume ⅡI*, Posts&telecommunications press, 2002.

[2] LÜ Hui, WU Chan-le, ZHOU Yi-qin et al, "A real-time Multicast in Multimedia Distance Education Network.J," *Wuhan Univ.(Nat.Sci.Ed.)*,1999,45(5): 531~534.

[3] Pusateri T, "Distance Vector Multicast Routing Protocol,"http://www.ietf.org/intern-et-drafts/draft-ietf-idmr-dvmrp-v3-11.txt,2000,8.

[4] Tony Ballardie, "Core Based Trees (CBT) Multicast Routing Architecture," http://w-ww.ietf.org/rfc/rfc2201.txt,1997,7.

[5] Bill Fenner, Mark Handley, Hugh Holbrook et al, "Protocol Independent Multicast-Sparse Mode(PIM-SM): Protocol Specification(Revosed)," http://www.ietf.org/internet-drafts/draft-ietf-pim-sm-v2-new-11.txt,2004,10.

[6] Deering S ,Cheriton D, "Multicast routing in datagram

internetworks and extended LANs," *ACM Transaction on Computer Systems*, 1990, 8(2): 85~110.

[7] Fujinoki H, Christensen K.J, "The directed reverse path join(DRPJ)protocol: an efficient multicast routing protocol," *Computer Communication*, 2001, 24: 1121~ 1133.

[8] Fujinoki H, Christensen K, "The new shortest best path tree (SBPT) algorithm for dynamic multicast tree," in *Proceedings of the IEEE 24th Conference on Local Computer Networks*,1999:204~211.

[9] Hui Lü, Yanxiang He, et.al, "The Balancing –Flow Reverse Path Join Protocol based-on Multicast," in *Proceedings of the 17th Conference on Parallel and Distributed Computing and Systems*, November 14-16,2005, Phoenix, AZ, USA: 454~458

[10] YAN Wei-Min, Wu WeiMin, *Data Structure*, Tsinghua University Press,2001.

A Path Collection Mechanism Based on AODV Protocol in Ad Hoc Network*

Jiande Lu[1], Zhenzhong Wang[1], Yuan Guan[2]
[1]Dept. of Computer Engineering, Soochow University
Suzhou, Jiangsu 215006, P.R.China
[2]Dept. of Elementary Education, China Pharmaceutical University
Nanjing 210009, P.R.China
Email: [1]lujiande@suda.edu.cn, [2]peacemay@163.com

ABSTRACT

An optimization scheme to AODV protocol through path collection is examined and proposed. This mechanism adopts the path collection scheme in DSR protocol to improve the performance of AODV, meanwhile it avoids being affected by the high running overhead and weak scalability of DSR protocol. Results obtained by Network Simulation (NS) shows that the optimized AODV mechanism performs effectively in terms of packet delivery ratio, routing overhead and end-to-end delay.

Keywords: AODV, DSR, AODV-PA, Path Collection, Ad Hoc Network

1. INTRODUCTION

The ad hoc on-demand distance-vector (AODV) is an on-demand dynamic routing protocol. The main advantages of AODV are: using the sequence number avoiding route looping; supporting intermediate nodes reply making the source node find routes fast; not carrying path information in the packet header to save network bandwidth; only storing the needed routes in nodes to decrease memory occupied; good expansibility.[1,2,3,5]

But to a certain extent, AODV's way of destination-oriented route searching limits the ability of finding out routes by the source nodes and results in many unnecessary route discovery procedures. To solve this problem, the designers of AODV proposed a protocol with path collection—AODV-PA[4] (AODV with path accumulation). It adopts the path collection scheme from DSR[7], and can find out more routes in one route discovery procedure and reduce the amounts of route requests obviously. This protocol suits for the networks whose data transfer requests are frequent. [2] But AODV-PA also introduces the disadvantages of DSR including: taking additional information in control packets bring larger overhead; adding RREQ and RREP processing in each node causing the longer processing time and the response time to route requests.

This paper proposes another path collection mechanism based on AODV—AODV-PC (AODV with Path Collection) that aims for promoting performance of AODV and keeping away from the disadvantages of DSR after adopting path collection scheme of DSR. This paper, at first, analyses the limits of AODV's ability to search routes and examines the scheme of AODV-PA to solve these problems, then illustrates the design of AODV-PC in detail, and simulates these three protocols in NS2 platform in different scenes. Simulation results show AODV-PC has the best performance and efficiency compared to AODV and AODV-PA in packet delivery ratio, routing overhead and end-to-end delay.

*The research of this paper has sponsored by the "211 Project" Key Construction Subjects Fund for the item of New Techniques of Computer Information Processing of Soochow University.

2. OVERVIEW OF AODV AND AODV-PA

2.1 AODV

The AODV is an on-demand dynamic routing protocol that uses routing tables with one entry per destination. All routes will be discovered only when needed. When a source node needs sending packets to a destination and there is no route to this destination in the source node's routing table, it generates a Route Request (RREQ) message and broadcast it. The destination or any other intermediate node that has a current route to the destination in its routing table would send back a Route Reply (RREP) message to the source node.

When an intermediate node receives a RREQ message, first, it will update its routing table for a reverse route to the source if necessary, then if the route to the destination exists in its routing table, it will generate a RREP message and unicast it to the next hop toward the source, otherwise the received RREQ message will be broadcasted again. Similarly, the forward route to the destination will be updated if necessary when an intermediate node receives a RREP message, and the RREP message will be unicast to the next hop toward the source, as indicated by the reverse route.

In AODV, the nodes maintain local connectivity by broadcasting local Hello messages or listening for packets from its set of neighbours. If a node does not receive any packets from its neighbour for more than one period of time, the node should assume the link to this neighbour is currently lost, and a Route Error (RERR) will be generated and sent to all its precursors that communicate over the broken link with the destination.

The AODV on-demand approach minimizes routing table information because each node stores only one path per destination and obtains just one route in a route discovery procedure. However, this potentially leads to a large number of route requests being generated.

As an example, consider nine nodes S, A, B, C, D, E, F, G and D shown in Fig.1.Node S wants to send data to node D. Since S does not have a route to D in its routing table, it broadcasts a RREQ message. A receives the RREQ message, updates its routing table for the reverse route to S if necessary, and forwards the request since it also has no route to D. Similarly, the RREQ message is processed by the nodes E, F, G, B and C. When a RREP message is generated by a node, say node D, it unicasts RREP message to the next hop in the reverse route -- node C. Node C receives the RREP message, updates its routing table for the forward route to D, and sends RREP to the next hop in the reverse route – node B. Similar process in the node B, A, G, F and E. When this cycle is

completed, the node S, A, B, C, E, F, G and D just obtain the route to S and D, but all the routes to the intermediate nodes such as A and B can not be obtained by this route discovery procedure. To improve the performance of AODV, Sumit Gwalani Elizabeth M. Belding-Royer and Charles E. Perkins modified AODV and published AODV-PA. [4]

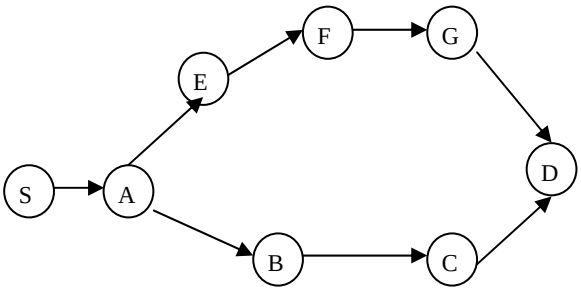


Fig.1. A Simple Network Topology

2.2 AODV-PA

AODV with Path Accumulation (AODV-PA) modifies the AODV to enable path accumulation during the route discovery cycle. This method of path accumulation is similar with Dynamic Source Routing (DSR) [7]. When the RREQ and RREP messages are generated or forwarded by the nodes in the network, each node appends its own address on these route discovery messages. So the RREQ and RREP packets contain a list of all the nodes traversed. Each node also updates its routing table with the information of the traversed nodes contained in the control messages. So after a source node establishes route to a destination node, it also establishes routes between the end node and the intermediate nodes.

As shown in Fig.1, for example, the node S broadcasts a RREQ message to query node D. When the RREQ message passes node A, node A updates its routing table for the reverse route to S and appends its own address to the RREQ packet and then forwards it. Node B receives the RREQ message, it updates its routing table for the reverse route to S and A, before forwarding, it appends its own address to the RREQ packet. Similarly node C updates the routing table for route to S, A and B, while D updates the routing table for route to S, A, B and C. The same things occurres with RREP message.

When the source node S has built its route to the destination D, it has also learnt the routes to the intermediate nodes. So if the source node has the requirements of communication with these intermediate nodes, it does not need to start another route discovery procedure so as to decrease the number of route discovery procedures as compared to basic AODV. This design scheme increases the efficiency of AODV. However, there are three primary disadvantages of AODV-PA. First, it increases the delay of route query. Second, most of the discovered routes in a discovery cycle are unidirectional routes, just reverse routes. Third, the route request packets flooding results in costly MAC layer overhead.

3. OPTIMIZATION DESIGN IN AODV-PC

As the processing in the path collection scheme of DSR, if each node, after normal processes of RREQ and RREP messages, needs to additionally deal with the intermediate nodes information gathering, the scheme will delay the route discovery procedure, and the large packets flooding will increase the network overhead. Thinking of these problems, AODV can be optimized with the path collection mechanism in such a way: when AODV completes route discovery procedure, a control packet is sent to collect path information. With this method, AODV would not delay routing process, but also can establish more routes along the optimization path, and the control packet gathering path information unicasts and this would not increase network overhead as flooding. In this optimized scheme, the source node and the destination node initialize the route collection procedure respectively and establish bidirectional routes between source and destination.

Based on above analysis, this paper proposes another path collection mechanism—AODV-PC (AODV with Path Collection). The mechanism keeps the control packet types and route discovery procedure of AODV and adds the following processing:

If the destination node replies a RREP message, after sending RREP, the destination node sends a CRREP message to source node. Fig.2 shows the packet format of CRREP, the additional field is used to gather the information of intermediate nodes along the path. The node receiving CRREP message updates or creates the routes to the nodes between the destination node and itself according to the CRREP additional field, and appends itself to the end of the additional field. After source node receives RREP message, it will also sends CRREP message to the destination node and each intermediate node processing is the same.

If the intermediate node replies a RREP message, then the source node will sends CRREP message to the destination node after it receives RREP from the intermediate node. The destination node will also send CRREP message to the source node after it receives the unpaid RREP message, and all the intermediate nodes processing to CRREP is the same as above.

Type	Reserved	Hop Count
Destination IP Address		
Destination Sequence Number		
Path Node IP Address		
Path Node Sequence Number		
(additional path node IP address and sequence number pairs)…		

Fig.2. The Format of CRREP

In order to illustrate AODV-PC mechanism, we take an example as the following. As shown in Fig.1, the node S broadcasts a RREQ message to query node D. When D receives RREQ message it will send back a RREP message and a CRREP message to node S along the reverse route, and record every intermediate node IP in CRREP. The source node also sends a CRREP message to the destination node after it receives RREP. Each node receiving a CRREP message appends itself to the CRREP's additional field and forwards this CRREP message. When CRREP message goes through node B, it adds route to node C into routing table, and when CRREP message goes through node A, it will add routes to node B and C into routing table, and in the end when CRREP goes to node S, it will add routes to A, B and C into routing table.

In another case, if RREQ broadcasts to an intermediate node, say node B, and there is a route to D in B's routing table, then B sends RREP to the source and destination node. After the source node receives RREP or the destination node receives unpaid RREP, they will send CRREP message. The intermediate nodes receiving this CRREP message process in the same way as above. After this procedure, the routes from node S to node D and to each intermediate node are established.

4. SIMULATION AND PERFORMANCE ANALYSIS

4.1 Simulation Environment And Test Factors

To Study the performance of AODV-PC, this paper uses the NS2 platform to simulate the AODV-PC, AODV-PA and AODV, and compares their performances and efficiencies based on the simulation results. The standard AODV protocol uses the aodv-uu 0.8 source code. (developed by Uppsala University), the AODV-PC and AODV-PA source codes are developed by modifying the aodv-uu 0.8 code.

The simulation environment is free space module, and there are 50 nodes randomly placed on a rectangular 1000 m * 1000m area. The transmission range of each node is 250 m. The max number of connections from source to destination is 20 and the packet sent rate at source node is 2 packets/s. Data streams use TCP or CBR (continuous bit-rate), the packet size of CBR is 512 byte. The different five speeds of mobile nodes are 0 m/s, 5 m/s, 10 m/s, 15 m/s and 20 m/s in five scenarios. Once the destination is reached a position, another random destination is targeted after a 30s pause. The total simulation time is 500s, and each data point in the follow figures is the average of 3 runs with the same scenarios configuration but different random seeds.

The factors to estimate the routing protocols' performances are: Routing Overhead which is the number of control packets, Packet Delivery Ratio which is the number of packets received by all of the nodes divided by the number of packers sent by all of the nodes, End-to-End Delay which is the average travel time of packets from source to destination.

4.2 Simulation Results Analysis

- **the Routing Overhead**

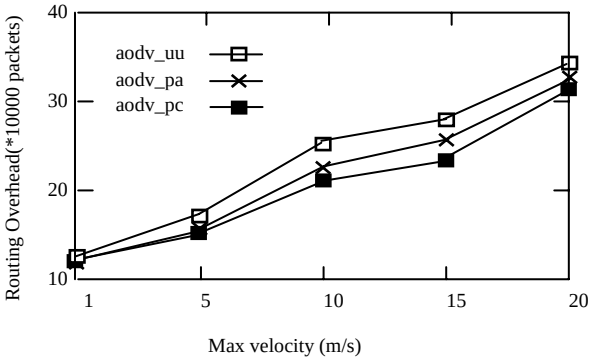


Fig.3. Routing Overhead of CBR

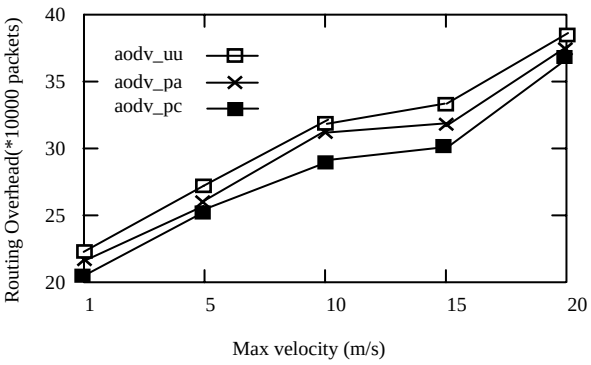


Fig.4. Routing Overhead of TCP

Fig.3 and Fig.4 show the comparison of the three protocols' routing overheads under different nodes' mobile speeds. As shown in these two figures, the overheads of the three protocols are increased while the nodes' mobile speeds become higher. This is because while the nodes move more quickly, the links break more frequently, the probability of exiting routes being useless is promoted, so the times of route discovery procedures increased. Between the three protocols, AODV-PC and AODV-PA are obviously better than AODV. Because the path collection scheme lets routing protocols can find more route information and reduce times of the route discovery procedures, so results in less overhead.

Although the AODV-PA's control packet size is larger, its number of control packets is much less than AODV. The cost of lots packets to snatch channels is larger than the cost of long packets, [6] so AODV-PA is more efficient than AODV in routing overhead factor. Between the two better protocols, AODV-PC is better than AODV-PA, this is because AODV-PC not only uses CRREP packet to collect route information and reduce overhead but also uses unicast way to transmit CRREP packet and reduce the routing overhead. When data steams uses TCP, the AODV-PC's advantage is more obvious. AODV-PA can find more route information than AODV-PC, but the excessive routes established are unidirectional routes. When one sender sends TCP segments through these routes, the receiver needs to initiate route discovery procedure to find the sender, so the routing packets of AODV-PA is not less than AODV-PC's, plus the advantage of less packets' size, AODV-PC is better than AODV-PA in routing overhead factor.

- **Packet Delivery Ratio**

Fig.5 and Fig.6 show the comparison of the three protocols' packet delivery ratio under different nodes' mobile speeds. While the nodes' mobile speeds become higher, the links break more frequently and packet delivery ratios of the three protocols go down. AODV-PC and AODV-PA's packet delivery ratios are better than AODV's. This is because the frequent changing topology results AODV needs more control packets to find the broken routes, this increases the failing transfer ratio caused by collisions. And AODV-PC is more efficient than AODC-PA in packet delivery ratio factor. Because AODV-PA uses RREQ and RREP to carry path information, this results RREQ packets' size becoming larger continually flood in whole network, make more collisions and lower packet delivery ratio.

When data streams uses TCP, the packet delivery ratio is very high because of TCP's reliable data transfer, and the failings are just caused by topology changes. AODV-PC is also little

better than AODV-PA, because AODV-PA's control packets are not less than AODV-PC's and AODV-PA's larger packets' size is easier to make collisions as described in previews.

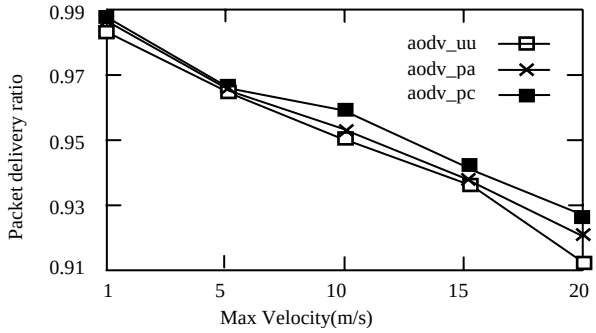


Fig.5. Packet Delivery Ratio of CBR

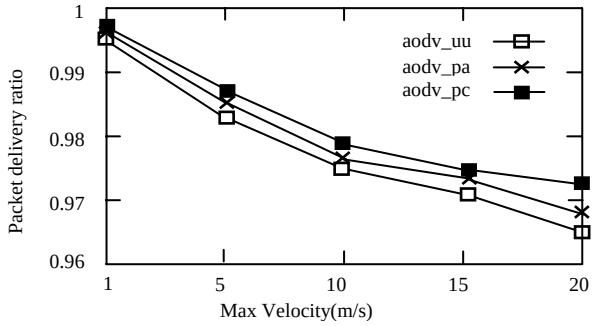


Fig. 6. Packet Delivery Ratio of TCP

- **End-to-End Delay**

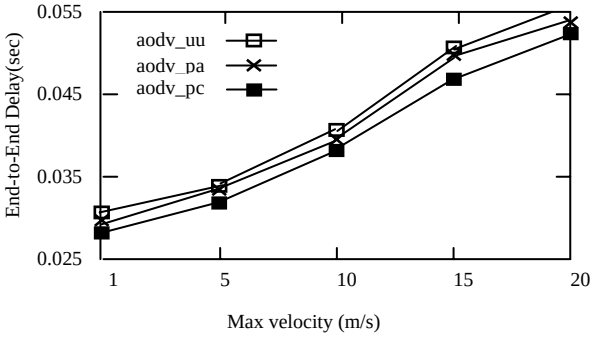


Fig.7 End-to-End Delay of CBR

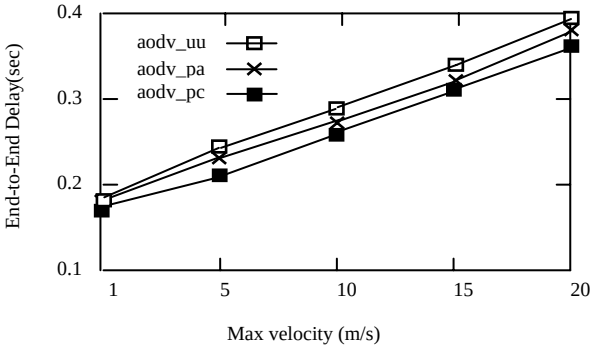


Fig.8. End-to-End Delay of TCP

Fig.7 and Fig.8 show the comparison of the three protocols' eng-to-end delay under different nodes' mobile speeds. As shown in these two figures, the end-to-end delays of the three protocols are increased while the nodes' mobile speeds become higher. This is because while the nodes move more quickly, the links break more frequently, the waiting time of data transfers is longer, so the end-to-end delay becomes longer. Compared to AODV, the efficiency of AODV-PC and AODV-PA is better. Because AODV needs more route discovery procedures to find new routes and the waiting time to deliver data packets is longer. The path collection scheme lets AODV-PC and AODV-PA can find more routes in one route discovery procedure and some data packets can transmit along these route paths, so it shortens the end-to-end delay.

Because of longer time to establish route in AODV-PA than in AODV-PC, the waiting time of data packets in senders is longer in AODV-PA, so the efficiency of AODV-PC's end-to-end delay is better than AODV-PA's. As described in 4.2.1 and 4.2.2, the advantage of AODV-PC is more obvious when data using TCP. In end-to-end delay factor this conclusion also stands.

5. CONCLUSIONS

This paper proposes a routing mechanism called AODV-PC which imports the path collection scheme from DSR protocol to AODV protocol, lets AODV establish more routes in one route discovery procedure. Simulation results show that this paper's optimized mechanism have better performance in packet deliv- ery ratio, routing overhead and end-to-end delay than another path collection mechanism—AODV-PA. The paper is with a view to promoting performance of AODV, and while AODV protocol becoming more and more perfect, it will play a more important role in future MANET application.

REFERENCES

[1] Elizabeth M. Belding-Royer, Charles E. Perkins , "Evolution and Future Directions of The Ad Hoc On-demand Distance-Vector Routing Protocol [J],"in *Ad Hoc Networks*, 2003(1),pp125-150.

[2] S. R. Das, C. E. Royer, M. K. Marina, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks[A],"in *IEEE Personal Communication Magazine special issue on Ad Hoc Networking*, Feb 2001,pp16-28.

[3] C. Perkins, E. Royer, and S. Das, *Ad Hoc On Demand Distance Vector (AODV) Routing [Z]*. RFC 3561, July 2003.

[4] S. Gwalani, Elizabeth M. Belding-Royer. AODV-PA: AODV with Path Accumulation *[A]*. *Proceeding of the IEEE Symposium on Next Generation Internet (NTI)*. AK: Anchorage, May 2003.

[5] Charles E. Perkins, Elizabeth M. Royer. *Ad hoc On-Demand Distance Vector (AODV) Routing[Z]*. draft-perkins-manet-aodvbis-01.txt, IETF internet draft, Jan 2004.

[6] J. Broch, D. A. Maltz, D. B. Johnson, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Newwork Routing Protocols [A]," in *Proceeding of the 4th International Conference on Mobile Computing and Networking*, Texas: Dallas,Oct.1998,pp85-87

[7] D. B. Johnson and D. A. Maltz,“ Dynamic Source Routing in Ad Hoc Wireless Networks,” in *T. Imielinski and H. Korth, editors,Mobile Computing*, vol.353, pp153–181, Kluwer Academic Publishers, 1996.

A Stability Based Routing Protocol in Ad Hoc Networks*

Kunpeng He ， Layuan Li
School of Computer Science and Technology, Wuhan University of Technology
Wuhan, Hubei , China
Email: hkp974120@sohu.com

ABSTRACT

Majority of the routing protocols proposed till date are based on the hop-count metric. Hop-count based protocols try to find a shortest path to destination. However, this metric is not fully applicable to the Ad Hoc Networks that Mobile node due to topology changes. Around this issue, with the conception such as older links more stable which used in ABR, we propose a stability based routing protocol SAODV using AODV as the basic routing protocol, this protocol use routing stability as a metric to select route and the goal is to find a longer survival time of route, simulation results show that SAODV better than AODV in packet delivery fraction, routing load and other aspects.

Keywords: AODV, SAODV, Stability, Routin Protocol

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) [1] is a wireless network consisting of mobile nodes, which can communicate with each other without any infrastructure support. In these networks, nodes typically cooperate with each other, by forwarding packets for nodes which are not in the communication range of the source node.

Typically, routing protocols are classified according to the route discovery philosophy, into either reactive or proactive. Reactive protocols are on-demand. Route-discovery mechanisms are initiated only when a packet is available for transmission, and no route is available. The proposed on-demand routing protocols include an ad-hoc on-demand distance vector routing (AODV) [2], dynamic source routing (DSR) [3], temporally ordered routing algorithm (TORA) [4], signal stability routing (SSR) [5], associativity-based routing (ABR) [6], and location-aided routing (LAR) [7]. On the other hand, proactive protocols are table-driven. Routes are precomputed and stored in a table, so that route will be available whenever a packet is available for transmission. Table-driven routing protocols include destination sequenced distance vector routing (DSDV) [8], cluster-head gateway switch routing protocol (CGSR) [9,10], wireless routing protocol (WRP) [11], adaptive distance vector routing (ADVR) [12]. In our work, we see the classification from a different perspective.

We classify routing protocols on the basis of metrics considered by them. We broadly classify routing protocols into hop-count based, and stability based. Each of these classes of routing protocols can be either proactive or reactive. Majority of the routing protocols proposed till dates are based on the hop-count metric. Hop-count based algorithms typically try to optimize the length of the route. Another category based on link stability is unique to wireless network. Link stability refers to the ability of a link to survive for certain duration. The higher the link stability, the longer is the link duration. The stability of a link depends on how long two nodes, which form that link, remain as neighbors. Two nodes are neighbors when they remain within each other's communication range, or the signal strength is above certain threshold. Mobility causes link breakage and leads to route recovery. A more stable link should therefore be preferred. A crucial issue with stability based routing algorithm is that much longer routes can be obtained compare to hop-count based routing.

In this paper, we propose a protocol called stability based routing protocol SAODV that considers stability metric. SAODV uses AODV (which is hop-count based) as the basic routing protocol and uses hello message mechanism computing link stability. Simulation results show that SAODV performs better than AODV.

The remainder of this paper is organized as follows. In Section 2, we present related work on stability based routing protocol. Section 3 describes an SAODV routing protocol in detail. Performance evaluation via simulation is presented in Section 4 and the conclusion is drew in Section 5.

2. RELATED WORK

As many popular MANET routing algorithms are hopcount based, we will present related work on stability based routing protocols in this section.

Path stability depends on the availability of all the links constituting the path. A link is available when the radio quality of the link satisfies the minimal requirement for a successful transmission. Stability based protocols use stability as the routing metric. The implicit goal of most stability based routing protocols is to find and select the longest lived routes. The difference lies in how the stability of a link is estimated and how these link estimates can be combined to form end-to-end estimates.

Associativity Based Routing (ABR) [6] is probably the first protocol in the class of stability based protocols for MANETs. In ABR, a new metric called associativity is defined to determine link stability. In simple terms, ABR is based on the idea that nodes which are neighbors for a threshold period are more likely to remain as neighbors for longer time, or less likely to move away. ABR assumes that after the threshold period, nodes move with similar speeds and directions and tend to stay together.

Signal Stability based Adaptive (SSA) [5] is a routing protocol, which finds route based on signal strength and location stability. In SSA, a mobile node measures the signal strength received from other nodes, and this information is used to estimate the link stability between them. The location stability mechanism is considered only as a supplement to signal-strength measurements. Simulation results in [5] shows that the performance of SSA with location stability

*Support by: Nature science foundation of China (No.60672137) and Specialized Research Fund for the Doctoral Program of Higher Education (No. 2006497015)

mechanism is not much better than a simple shortest path algorithm.

The protocol RBAR[13] is an extension to SSA which assigns a threshold to the level of signal-strength and based on this threshold choose the routes. This protocol suffers from the disadvantage of having to choose the optimal threshold values. stability and hop-count based routing algorithm (SHARC) [14] is a algorithm which using DSR as the basic routing protocol. which finds the most stable route among the set of shortest hop routes. The stability of a path is calculated using a simple histogram based estimator. Performance evaluation of SHARC shows that it performs better than purely stability based and purely hop count based algorithms in terms of throughput of long-lived flows and response time of short data transfers.

In our work, we use AODV as the basic routing protocol is because AODV is a on-demand routing protocol, the performance of on-demand protocols are better than Table-driven routing protocols and AODV is better than other on-demand routing protocols in many aspects. We want to find a longest lifetime route among the set of shortest hop routes, but the simulation result demonstrate this method is no better than the one we proposed.

3. AN SAODV ROUTING PROTOCOL

3.1 Data Structures Used in Proposed Protocol

In order to calculate stability information and select a longer lifetime route, the route request (RREQ) packet, route reply (RREP) packet, route table entry and neighbor list of AODV is modified. Tables 1, Table 2, Table 3 and Table 4 show the modified format respectly.

Table 1. The format of RREQ

Type	Reserved	Hop Count
RREQ ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		
RQ_MDS		

Table 2. The format of RREP

Type	Reserved	Hop Count
RREP ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Life time		
RP_MDS		

Table 3. The format of neighbor list

Neighbor ID	Life time	NB_DS

Table 4. The format of route table entry

Rt seqno	Rt_next hop	Precursors list	Life time	Rt _MDS

We add RQ_MDS field in RREQ and RP_MDS field in RREP, the RQ_MDS field record the maximum value of stability between adjacent nodes the RREQ packet is through, and the RP_MDS records the maximum value of stability between the nodes the RREP packet is forwarded. The initial value of RQ_MDS and RP_MDS is 0. In SAODV, each node maintain a route table and a neighbor list, we add a RT_MDS field in route table entry, this field record the maximum stability of route which from source to destination. In neighbor list, we add a NB_DS field, which store the stability value with its neighbors.

3.2 Stability Estimator

In SAODV, The route to the destination is selected based on nodes having periods of stability. Period of stability is an interval in which a node is constantly associated with certain neighbors over time without losing connectivity with it. Each node generates a hello message and periodically broadcasts to signify its existence. For each hello message received, the NB_DS of the current node with respect to the neighboring node is incremented. A high degree of stability may indicate a low state of node mobility and vice versa. NB_DS are reset when the neighbors of a node or the node itself move out of proximity.

The link stability depend on the nodes receive numbers of hello message from its neighbor. And the selection of route stability based on the link stability, let $r(n_1, \ldots, n_n)$ is a path from n_1 to n_n, $Sr(n_1,n_n)$is the stability of path $r(n_1, \ldots, n_n)$, for any two adjacent nodes n_i,n_j. Suppose link $l(n_i,n_j)$ is between two adjacent node n_i,n_j. The stability of $l(n_i,n_j)$ is $Sl(n_i,n_j)$. So, the stability of $r(n_1, \ldots, n_n)$ is:

$$Sr(ni,nj) = \min Sl(ni,nj) \quad , \quad \{ n_i, n_j \in (n_1, \ldots, n_n) \}$$

The algorithm to lookup the stability of link(i,j) when i receive a hello message from j shown as follow:

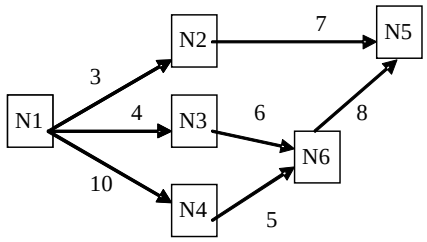
```
Algorithm: loopup_stability (addr)      //addr is address of j
Initial: nb = nbhead.lh_first. Where nb is a pointer,
nbhead.lh_first is pointer point to the first neighbor in i's
neighbor list.
WHILE nb is not null
      IF   address of nb is equal to addr
           Return   stability for j
      ELSE
           nb point to the next neighbor
      END IF
END WHILE
```

3.3 Route Discovery Process

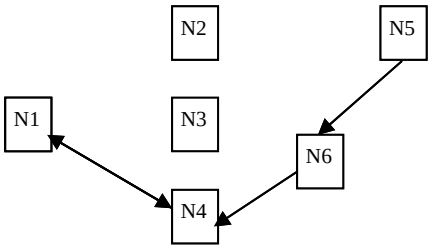
When a source needs to send a data packet to the destination, it will first check its routing table to see if it has an unexpired route to destination. If it does, it will send data packets using the route immediately. Otherwise it broadcasts generally known RREQ packet to find a route to the destination. Figure 1 depicts an example of the route setup process. In Fig. l(a), the source node N1 broadcast a RREQ packet to destination N5. N2, N3, N4 and N6 forward the RREQ packet and modify the stability value of the link that the packet was received from.

When the Intermediate nodes receive a RREQ packet, it will check if it received the same RREQ, if received, free this RREQ packet. Otherwise, the nodes will lookup the NB_DS of the neighbor that the packet was received from. And compare it with RQ_MDS field in RREQ, then store the larger one in RQ_MDS field. If a new route is offered to a node, the

node compares the destination sequence number for the new route to the destination sequence number for the current node. The route with the greater sequence number is chosen. If the sequence numbers are the same, then the new route is selected only if it has a larger stability metric. Except the work mentioned above, the intermediate node build the reverse route to source node yet, The reverse is used to forward the RREP packet.



(a) Broadcast RREQ



（b） Forward RREP

Fig.1. Route Discovery Process

In Fig.1(a), node N1 want to send data to N5, if N1 don't have route to N5, N1 will generates a RREQ packet and broadcast it, when N2,N3,N4 receive the RREQ packet, check whether received same RREQ packet, if not, search the stability value for N1 and build or update the route to the N1. If they have route to destination N5, they send RREP packet to N1, otherwise broadcast RREQ packet. When N6 received RREQ packet from N3 and N4, N6 select the route with higher stability (there is one route to destination in AODV). When N5 receive first RREQ packet, it will wait for a period of time to receive other RREQ packet. Finally, two RREQ packets arrived at node N5, One path contains <N1, N2, N5> with stability value 7 and the other path contains <N1, N4, N6, N5> with stability value 10. The destination node N5 selects a path <N1, N4, N6, N5> with larger stability value 10 to send RREP packet, Figure l (b) is the route reply process. Intermediate nodes receive the RREP packet use the same way update the route to the destination or establish the route to the destination that use to forward data packet.

The algorithm of intermediate node receiving RREQ as follow:

```
Algorithm: recevrreq( p ) //p is a RREQ packet

IF (( the address of node = source address in RREQ) OR
    (RREQ_ID exist in node's broadcast list))
      Discard RREQ
END IF
Lookup stability for the RREQ received from
IF (stability > RQ_MDS)
     RQ_MDS = stability
END IF
IF (the node have't route to source)
     Add a route entry to source in route table
ELSE
     IF ((route seqno > RREQ seqno) OR ((route seqno =
           RREQ seqno) AND (RT_MDS < RQ_MDS)))
        Update route entry to source
     END IF
END IF
IF (the node is the destination)
    Wait for a period of time to receive other RREQ
    Select the route have higher stability send RREP
ELSE
    Broadcast RREQ
END IF
```

In the course of modify the protocol, we select the average stability of nodes, the sum stability of nodes and the maximum stability of nodes on the path as the stability of path to simulate the protocol, we found that the third one as stability of path have better performance than the others.

4. PERFORMANCE EVALUATION

To test the performance of SAODV routing protocol, we use Network Simulation 2 (NS 2) [15] to conduct the simulation.

4.1 Simulation Environment

1) Propagation: TwoRayGround
2) Radio range of a node: 250 m
3) Channel capacity: 1 Mb/sec
4) Medium Access Control (MAC) protocol: IEEE802.11 Distributed Coordination Function (DCF)
5) Traffic pattern: 50 CBR/UDP
6) Size of data packet: 512 bytes
7) Data rate: 4 packet/sec
8) Simulation area: 600 m × 800 m
9) Number of nodes:40
10) Maximum speed: 20m/s
11) Pause time: 0s, 20s, 60s,150s,300s
12) Simulation time: 500 seconds
13) Routing protocol: AODV and SAODV

4.2 Performance Parameters

We evaluated the performance of SAODV by measuring four parameters: packet delivery fraction, normalized routing load, throughput and generate RREQ frequency.

(1) Packet delivery fraction: the ratio between the number of packets originated by "application layer" CBR sources and the number of packets received by the CBR sink at the final destination. Packet delivery ratio affects the maximum throughput that the network can support. This metric characterizes both the completeness and correctness of the routing protocol.
(2) Normalized routing load: the ratio between the total numbers of routing packet transmitted during simulation and the number of packets originated by "application layer" CBR sources. For packets sent over multiple hops, each transmission of a packet over a hop counts as one transmission. Protocols that generate large amounts of routing overhead increase the probability of packet collision and data packet delays in network interface queues.
(3) Throughput: the ratio between the bps received by the CBR sink at the final destination and the simulation time.
(4) Generate RREQ frequency: the ratio between the numbers of RREQ generated by all source and the

simulation time. It means the number of RREQ generated by all source per second.

4.3 Result and Analysis

Fig. 2 demonstrates the relationship of packet delivery fraction (pdf) and the node's pause time. As the pause time increases, packet delivery fraction in SAODV and AODV all increase, and increased value is dramatically. Simultaneously the packet delivery fraction of SAODV better than AODV. We will find that, when the node in high mobile environment (the pause time of node arrive a destination is short or it always in mobile state), the packet delivery fraction of SAODV is much higher than AODV. the route to the destination in SAODV is a longest survive time path, which more stable than the shortest path in AODV, when node transmits data packet under mobile environment, the numbers of discovery route in SAODV is less than AODV and SAODV will transmit more data packets than AODV.

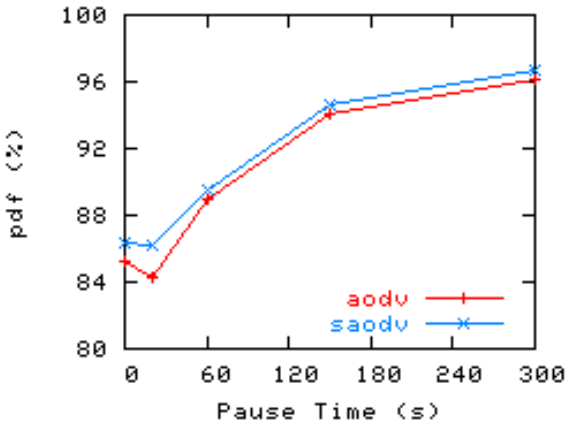


Fig.2. Packet Delivery Fraction

Fig. 3 shows the relationship of normalized routing load and the node's pause time. From Fig.4, normalized routing load decrease with the increase of node's pause time and the normalized routing load of AODV is higher than SAODV. in same environment routes become invalid more easily with AODV, thus AODV need more RREQ packet and RREP packet to discovery route, it will increase the network load.

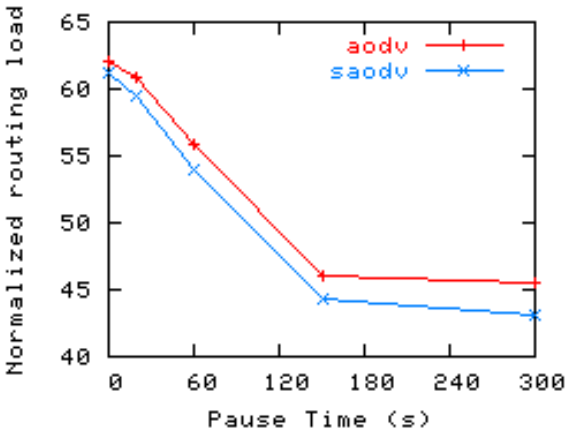


Fig.3. Normalized Routing Load

Fig.4 demonstrates the relationship of throughput and the node's pause time. As the pause time increases, throughput in SAODV and AODV all increase, we also see that, in high mobile environment, the throughput of SAODV is much higher than AODV, it is the same because stable route have longer lifetime than the short route. The packet delivery fraction is a important factor lead SAODV have higher throughput than AODV.

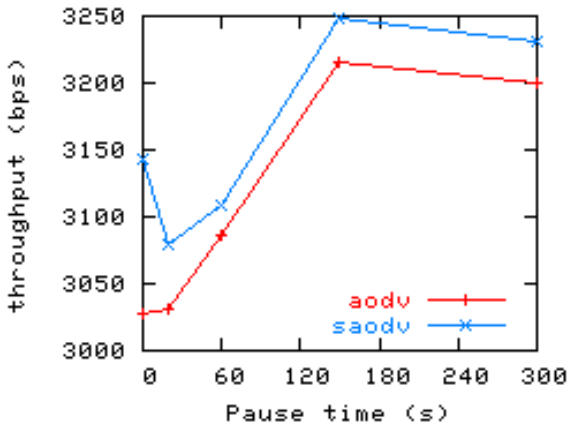


Fig.4. Throughput

Fig.5 demonstrates the relationship of generate RREQ frequency and the node's pause time. In Fig.5, the generate RREQ frequency of two protocols is decrease as the pause time increases. With the pause time decreases, much more available routes will be broken, and the number of route discoveries will increase rapidly. The generate RREQ frequency of SAODV is less than AODV 2~3 times per second. This is because SAODV select longest lifetime route in route discovery process, the number of available paths is more than AODV. Of course, it is more frequent for AODV to initiate route discovery.

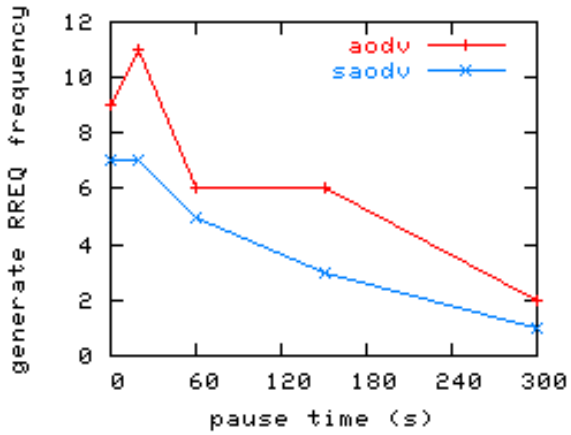


Fig.5. Generate RREQ Frequency

5. CONCLUSIONS

In this paper**,** we presents a stability based routing protocol SAODV, SAODV is a protocol which modified the RREQ packet, RREP packet, neighbor list, route table entry and route discovery process of AODV. The SAODV use hello message to calculate link stability, the stability used to find a longest survive time route in route discovery process. We introduce NS2 to simulate the protocol. Which evaluate performances of the packet delivery fraction and normalized routing load. As a result, the SAODV could enhance the packet delivery fraction and reduce the normalized routing load. In future work, more information of node and network will be added into protocol in order to fit the real MANET environment

REFERENCES

[1] Li Layuan and Li Chunlin, Computer NetWorks, Bei Jing: Defense Industry Press Pub., 2004, pp.145.

[2] C.E.Perkins and E.M.Royer, Ad-hoc On Demand distance Vertor Routing, Proceedings of the 2nd IEEE Workshop on Mobile computing Systems and Applications, New Orleans, LA, Feb 1999, pp.90~100.

[3] Johnson D.B. and Maltz D. A., Dynamic Source Routing Algorithm in Ad-Hoc Wireless Networks, Mobile Computing, Chapter 5, Kluwer Academic, Boston, MA, 1996, pp.153~181.

[4] V.D. Park and M.S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile and wireless networks," Proceedings of IEEE INFOCOM'97, Kobe, Japan, April 1997, pp. 103~112.

[5] R. Dube, C. D. Rais, K. Y. Wang and S. K. Tripathi. Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks, IEEEPersonal Communications Magazine, Feb. 2001.

[6] C-K and Toh. "Associativity-Based Routing for Ad Hoc Mobile Networks," International Journal on Wireless Personal Communications, Vol. 4 No. 2, March 1997, pp. 103~139.

[7] Ko Young-Bae and Vaidya Nitin H., "Location-Aided Routing in mobile ad hoc networks," Wireless Networks 6, 2000, pp.307~321.

[8] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing(DSDV) for Mobile Computers, ACM SIGCOMM ' 94 Conference on Communications Architectures, Protocols and Applications, London, England, August 1994, pp.234~244.

[9] C.C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proceedings of IEEE SICON, April 1997, pp.197~211.

[10] Li Layuan and Li Chunlin, A routing protocol for dynamic and large computer networks with clustering topology [J], Computer Communications, Vol. 23 No. 2 2000, Elsevier, UK, pp.171-176.

[11] T. W. Chen and M. Gerla, Global State Routing:A New Routing Scheme for Ad-hoc Wireless NetWorks （Wireless Routing Protocol, WRP）, Procedings of the IEEE Inernationsl conference on Communications(ICC), Atlanta, GA, June 1998：171~175.

[12] R.V. Boppana and Konduru, "An adaptive distance vector routing algorithm for mobile, ad hoc networks," INFOCOM 2001, Proceedings. IEEE, Vol.3, 2001 pp.1753~1762.

[13] S. Agarwal, A. Ahija, J. P. Singh and R. Shorey, "Route-lifetime Assessment Based Routing protocol for Mobile Ad Hoc Networks," Proceedings. IEEE International Conference on Communications, 2000, Vol.3, pp. 1697~1701.

[14] V.N.Sastry and P.Supraja, Stability and Hop-Count based Approach for Route Computation in MANET, Wireless and Mobile Computing, Networking and Communications, Proceedings. *IEEE International Conference on Communications*, August 2005, vol.3, pp.49~56.

[15] The Network Simulator - ns-2, June 2007.

Kunpeng He (1982-) is a master of School of Computer Science and Technology, Wuhan University of Technology. She graduated from Wuhan University of Technology in 2001 with specialty of computer networks. Her research interests are High-performance computer networks and protocols.

Layuan Li, was born in Hubei, China on 26 February 1946.He received the BE degree in Communication Engineering from Harbin Institute of Military Engineering, China in1970 and the ME degree in Communication and Electrical System from Huazhong University of Science and Technology ,China in 1982. He academically visited Massachusetts Institute of Technology (MIT),USA in 1985 and 1999, respectively. Since 1982,he has been with the Wuhan University of Technology (WUT), China, where he is currently a professor and Ph.D tutor of Computer Science, and editor in chief of the Journal of WUT. He is Director of International Society of High-Technol and paper reviewer of several IEEE Transactions and Jounals. He was the head of the Technical Group of Shaanxi Lonan PO Box 72,Ministry of Electrical Industry, China from 1970 to 1978. His research interests include computer networks, protocol engineering and image processing. Professor Li has published over one hundred and fifty technical papers and is the author of six books. He also was awarded the National Special Prize by the Chinese Government in 1993.

Comparison of Distributed Particle Filter for Passive Target Tracking in Wireless Sensor Networks *

Feng Xue, Genpeng Zhang, Zhong Liu
Electronics Engineering College Naval University of Engineering
Wuhan, Hubei 430033, China
Email: xfmilk@sohu.com

ABSTRACT

Two distributed particle filters for improving the passive tracking performance and balancing communication amount in wireless sensor networks (WSN) are proposed and compared with other schemes. Based on dynamic clustering, the information particle filter (IPF) receives observations from child nodes (CN) and formulates local estimates on head nodes (HN), which act as the processing center. On a HN, the parallel particle filter (PPF) divides the particle set into several subsets, which are distributed to CNs in the cluster, and processes of sub-particle filters run parallel using particle subsets. Computer simulations are conducted to compare tracking performance and to analyze communication amount overhead. Simulation results show that the IPF and the PPF have better tracking performance than the scheme based on the extended Kalman filter, and that two distributed particle filters balance and reduce communication amount overhead due to the distributed data exchange.

Keywords: Distributed Computing, Target Tracking, Passive Tracking, Maneuvering Target, Sensor Networks.

1. INTRODUCTION

Wireless sensor networks (WSN) technology is a key technology for the future, and recent advances in electronic and wireless technologies have greatly improved processing and communication capacities of WSN [1]. One of the most important application in WSN is target tracking. In military applications, stealthy operations require sensor nodes of WSN to obtain the bearings information passively. However because of the energy constraint of micro sensors, traditional tracking algorithms must be adapted to deal with special problems in WSN.

It is well known that particle filters (PF) are very suitable for non-linear and/or non-Gaussian applications [2]. Hence, high accuracy state estimates can be obtained by the PF applied in the passive tracking. However, if the PF is used directly in a fusion centre to process all observations from other nodes in WSN like the centralized particle filtering (CPF) algorithm, unbalanced communication and computation will cost the limited energy of the central node quickly, which will lead to power failure [3]. Distributed particle filters can balance the energy cost and improve the performance of passive tracking in WSN [4, 5].

In this paper, two distributed particle filtering algorithms are proposed and compared for tracking a target maneuvering through WSN. Based on the structure of dynamic clusters, head nodes (HN) receive observations from their child nodes (CN), and the information particle filter (IPF) is used to obtain local estimates on HNs. The particle set is divided into subsets processed by the parallel particle filter (PPF) on CNs in the cluster distributively. Positions of HNs change according to the position of the target, and local estimates are transmitted between HNs. The goal of these two particle-filtering algorithms is to perform high-accuracy, distributed estimation of target states on multiple sensor nodes, whilst attempting to balance communication overhead and to reduce computation on the central node. Computer simulation results have shown that not only the tracking accuracy is improved but also the average energy cost is balanced by the IPF and the PPF in WSN.

* This work was supported in part by the National Defense Funds of China under Contract No. 513040303.

2. DISTRIBUTED DYNAMIC CLUSTERING SCHEME

To balance the energy cost in WSN, we propose a new dynamic clustering scheme for tracking application. Sensor nodes are organized into clusters, in which HNs are elected to collaborate with other CNs. HNs are responsible for processing data to obtain local state estimates, while other CNs process their own observations independently. The dynamic changing of clusters can be decided by

$$\begin{cases} D + r < R & \text{Cluster generation and maintenance} \\ D + r = R & \text{Critical point of cluster changing} \\ D + r > R & \text{New cluster creation} \end{cases}$$

where D denotes the distance from the target to the HN, and r is the one-hop communication range decided by the energy cost of nodes, and R the maximal observable range of sensor nodes. As shown in Fig.1, there are two types of virtual circles in the tracking scene of WSN. The cluster circle (CC) with radius r includes all CNs in the cluster, and the sensing circle (SC) with radius R denotes the sensing area of the cluster.

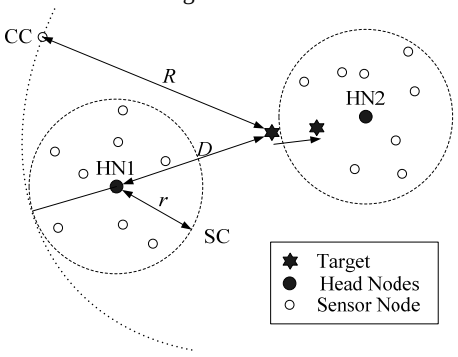


Fig.1. Dynamic cluster generation and destroy

As the target moves with time, dynamic processes of cluster generation and destroy are described by

(1) When a target enters the detection region of a sensor node in WSN, the node is triggered by its sensor. Relevant information is broadcast to nodes in the immediate vicinity within one-hop communication distance.

(2) When the number of sensor nodes that have detected the target reaches the predefined number, at current sample time, the node with the most intense signal from the target

in its immediate neighborhood is chosen as the local HN.

(3) As the target moving, all nodes in the distance *r* from the HN are activated as CNs and collaborated with the HN on tracking the target.

(4) When the critical point of cluster changing is met, some CNs in the cluster may reach the maximal sensing range *R*. Then, the position of the target at next sample time is predicted through the assumed state evolution equation $p(\mathbf{x}_k \mid \mathbf{x}_{k-1})$.

(5) A new HN is elected based on the closest position to the predicted, and a new cluster is created as Step (2).

(6) Packets of target state estimates are transmitted between the old HN and the new one to follow the target movement. Then nodes in previous cluster go back to sleep.

(7) As the target moves, above processes repeat until the target leaves the detection region of WSN.

In this distributed structure, the dynamic clustering based on the wake/sleep scheme can balance the energy cost of sensor nodes. All observations on sensor nodes in the cluster are effective, thus redundant computation and communication are reduced. Distances between any NH and its CNs are smaller than one-hop communication distance, so relay communication in multi-hop is avoid largely, which saves limit energy of sensor nodes.

3. INFORMATION PARTICLE FILTER IN WSN

3.1 Passive Tracking Model

To describe the state space evolution of maneuvering target precisely, the tracking model is constructed by the turn rate [6]. Define the state vector as $\mathbf{x}_k = (r_{xk}, v_{xk}, r_{yk}, v_{yk}, \varepsilon_{k+1})$, and considering the two-dimensional passive tracking problem, discrete state and observation equations are given by

$$\mathbf{x}_k = \mathbf{\Phi}_{k/k-1}\mathbf{x}_{k-1} + \mathbf{\Gamma}\mathbf{w}_{k-1} \tag{1}$$

$$\mathbf{z}_k = \mathbf{h}(\mathbf{x}_k, \mathbf{v}_k) = \tan^{-1} r_{xk} / r_{yk} + \mathbf{v}_k \tag{2}$$

where transition matrix is

$$\mathbf{\Phi}(\varepsilon_k) = \begin{bmatrix} 1 & \sin(\varepsilon_k T)/\varepsilon_k & 0 & -(1-\cos(\varepsilon_k T))/\varepsilon_k & 0 \\ 0 & \cos(\varepsilon_k T) & 0 & -\sin(\varepsilon_k T) & 0 \\ 0 & (1-\cos(\varepsilon_k T))/\varepsilon_k & 1 & \sin(\varepsilon_k T)/\varepsilon_k & 0 \\ 0 & \sin(\varepsilon_k T) & 0 & \cos(\varepsilon_k T) & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The turn rate ε_k is assumed velocity-dependent according to the following model $\varepsilon_k = a_{typ} / \sqrt{v_{xk}^2 + v_{yk}^2}$, where a_{typ} is the typical manoeuvring acceleration, which is modelled as a set of three discrete values, having a Markovian switching structure.

3.2 Information Extended Kalman Filter for Passive Tracking

In the distributed passive tracking system, the extended Kalman filter can not be used directly to obtain the sensor fusion. Hence, with the assumption of Gaussian, Eq. (2) is linearized around $\hat{\mathbf{x}}_{k/k-1}$ by the information extended Kalman filter (IEKF). The information matrix $\mathbf{U}_{k/k}$ is the inverse of the covariance matrix $\mathbf{U}_k = \mathbf{P}_k^{-1}$. The information vector $\mathbf{u}_k$ can be computed by the transformation from state to information space $\mathbf{u}_k = \mathbf{U}_k \hat{\mathbf{x}}_k$. The information propagation coefficient is given by

$$\mathbf{L}_{k/k-1} = \mathbf{U}_{k-1}\mathbf{\Phi}_{k/k-1}\mathbf{U}_{k-1}^{-1} \tag{3}$$

Predicted information vector and matrix are

$$\hat{\mathbf{u}}_{k/k-1} = \mathbf{L}_{k/k-1}\hat{\mathbf{u}}_{k-1} \tag{4}$$

$$\mathbf{U}_{k/k-1} = \mathbf{\Phi}_{k/k-1}\mathbf{U}_{k-1}^{-1}\mathbf{\Phi}_{k/k-1}^T + \mathbf{\Gamma}_{k-1}\mathbf{Q}_{k-1}\mathbf{\Gamma}_{k-1}^T \tag{5}$$

where $\mathbf{Q}_{k-1} = \mathrm{E}[\mathbf{w}_{k-1}\mathbf{w}_{k-1}^T]$. Consider a cluster with *N* CNs and a HN, the sum of information contributions due to *N* different sensors is

$$\mathbf{i}_k = \sum_{n=1}^{N} \mathbf{H}_k^T(n)\mathbf{R}_k^{-1}(n)\mathbf{z}_k(n) \tag{6}$$

$$\mathbf{I}_k = \sum_{n=1}^{N} \mathbf{H}_k^T(n)\mathbf{R}_k^{-1}(n)\mathbf{H}_k(n) \tag{7}$$

where $\mathbf{R}_k = \mathrm{E}[\mathbf{v}_{k-1}\mathbf{v}_{k-1}^T]$, and $\mathbf{H}_k$ is Jacobian matrix of $\mathbf{h}_k$. The updated information vector and matrix are

$$\hat{\mathbf{u}}_k = \hat{\mathbf{u}}_{k/k-1} + \mathbf{i}_k \tag{8}$$

$$\mathbf{U}_k = \mathbf{U}_{k/k-1} + \mathbf{I}_k \tag{9}$$

It is computationally easier to implement an IEKF in a WSN environment since it is simply sum of individual information contributions. However, the first-order approximation to nonlinear function can lead to poor performance of the passive tracking system. Hence, new distributed nonlinear filters should be adopted to improve the tracking performance in WSN.

3.3 Distributed Information Particle Filter

The PF provides a complete description of probability distributions involved in the estimation process and tends to improve the accuracy of passive tracking. However, the selection of the proposal density distribution is a main problem of the PF. If the state transition does not take into account the most recent observation, particles drawn from proposal density may have very low likelihood, and their contributions to the posterior estimation become negligible. Proposal density generation algorithms based on the Kalman filter can incorporate the most current observation with the optimal Gaussian approximation to states. Thus the IEKF is used to perform joint estimation using observation from sensors in the cluster and to generate the proposal density of the IPF, which can be given by

$$q(\mathbf{x}_k^i \mid \mathbf{x}_{0:k-1}^i, \mathbf{z}_{1:k}) = N((\mathbf{U}_k^i)^{-1}\hat{\mathbf{u}}_k^i, (\mathbf{U}_k^i)^{-1}) \tag{10}$$

where $N(\cdot)$ denotes the Gaussian distribution function. We assume that observations on individual nodes are independent conditioned on states. Hence, combined data likelihood for all sensors can be factored into products of data likelihoods on individual sensor nodes

$$p(\mathbf{z}_k^{1:N} \mid \mathbf{x}_k) = \prod_{n=1}^{N} p(\mathbf{z}_k^n \mid \mathbf{x}_k) \tag{11}$$

Thus, particle weights are computed by

$$w_k^i \sim \prod_{n=1}^{N} p(\mathbf{z}_k^n \mid \mathbf{x}_k^i) p(\mathbf{x}_k^i \mid \mathbf{x}_{k-1}^i) / q(\mathbf{x}_k^i \mid \mathbf{x}_{0:k-1}^i, \mathbf{z}_{1:k}) \tag{12}$$

Based on the dynamic clustering structure as Section 2, the implementation of distributed IPF algorithm is detailed below.

(1) Initialization.
A cluster is generated at initial sample time (*k*=0), and the HN draws particles from the prior $\mathbf{x}_0^i \sim p(\mathbf{x}_0)$ $i = 1,...M$

(2) Upload communication.
At sample time *k*, observation data from each CN are transmitted to the HN.

(3) Particle updating on HNs.
As previous particle set $\{\mathbf{x}_{k-1}^i, \mathbf{P}_{k-1}, w_{k-1}^i\}$ is known, each particle is updated by the IEKF from Eq. (3) to Eq. (9). The new updated information set $\{\hat{\mathbf{u}}_k^i, \mathbf{U}_k^i\}$ is obtained.

(4) Particle sampling on HNs.

The particle $\tilde{\mathbf{x}}_k^i$ is sampled from the proposal distribution via Eq. (10).

(5) Weight computing on HNs.
Importance weights are evaluated by Eq. (12), and the normalized process is performed to obtain $\tilde{w}_k^i$.

(6) Estimation on HNs.
On the HN, state estimates are computed by

$$\hat{\mathbf{x}}_k = \mathrm{E}[\mathbf{x}_k \mid \mathbf{z}_{1:k}] \approx \sum_{j=1}^{M} w_k^i \mathbf{x}_k^i \qquad \mathbf{P}_k = \sum_{i=1}^{M} (\mathbf{U}_k^i)^{-1} - \hat{\mathbf{x}}_k \hat{\mathbf{x}}_k^{\mathrm{T}} \quad (13)$$

(7) Resampling on HNs.
If the effective particle number gets lower than a given threshold, the particle set is resampled by

$$\{\tilde{\mathbf{x}}_k^i, \tilde{w}_k^i\} \rightarrow \{\mathbf{x}_k^i, 1/M\} \quad (14)$$

(8) Particle exchange.
When a previous cluster is destroyed and a new one is generated (the critical point of the cluster changing is met), the particle set needs to be transmitted from the former to the latter. To reduce communication cost, the particle set is reconstructed by mean and variance using the Gaussian mixture model (GMM [7]) on the new HN.

4. PARALLEL PARTICLE FILTER IN WSN

In the PPF, the entire particle set is divided into small subsets, and *N* sub-PFs are distributed over CNs, where sub-PFs run parallel. n_j denotes the particle number on the node *j*, and $\{\mathbf{x}_k^{i,j}, w_k^{i,j}\}$ is the *i*-th particle at sample time *k*. The implementation of the PPF algorithm is detailed below.

(1) Initialization.
When the cluster is generated at initial sample time (k=0), n_j particles are allocated to the *j*-th CN and spread along the detection geometry in x-y space according to $p(\mathbf{x}_0 \mid \mathbf{z}_0)$.

(2) Particle sampling on HNs.
At sample time *k*, particle set at previous time has been obtained. States are predicted by the state evolution equation $p(\mathbf{x}_k \mid \mathbf{x}_{k-1}^{i,j})$, and the new particle set is sampled by

$$\mathbf{x}_k^{i,j} \sim q(\mathbf{x}_k \mid \mathbf{x}_{k-1}^{i,j}, \mathbf{z}_k) = p(\mathbf{x}_k \mid \mathbf{x}_{k-1}^{i,j}) \quad (15)$$

(3) Updating and aggregating on CNs.
When present observations are available, CNs compute weights of particles via

$$w_k^{i,j} \propto w_{k-1}^{i,j} \frac{p(\mathbf{z}_k \mid \mathbf{x}_k^{i,j}) p(\mathbf{x}_k^{i,j} \mid \mathbf{x}_{k-1}^{i,j})}{q(\mathbf{x}_k^{i,j} \mid \mathbf{x}_{k-1}^{i,j}, \mathbf{z}_k)} = w_{k-1}^{i,j} p(\mathbf{z}_k \mid \mathbf{x}_k^{i,j}) \quad (16)$$

Then, each CN computes aggregated data as follows

$$S_k^j = \sum_{i=1}^{n_j} w_k^{i,j} \qquad X_k^j = \sum_{i=1}^{n_j} \mathbf{x}_k^{i,j} w_k^{i,j} \quad (17)$$

$$G_k^j = \sum_{i=1}^{n_j} (w_k^{i,j})^2 \qquad P_k^j = \sum_{i=1}^{n_j} w_k^{i,j} \mathbf{x}_k^{i,j} (\mathbf{x}_k^{i,j})^{\mathrm{T}} \quad (18)$$

where X_k^j is the unnormalized local estimate, and S_k^j is the unnormalized weight. G_k^j and P_k^j are used to compute estimation errors and to control degeneration respectively.

(4) Upload communication.
Aggregated data (S_k^j, X_k^j, G_k^j, and P_k^j) are transmitted to he HN.

(5) Estimation.
State estimates are computed parallel on the HN and their CNs. The HN runs state estimation and sums weights from its CNs as follows

$$C_k = \sum_{j=1}^{N} S_k^j \quad (19)$$

State estimates and covariances are computed by

$$\hat{\mathbf{x}}_k = \mathrm{E}[\mathbf{x}_k \mid \mathbf{z}_{1:k}] \approx \sum_{j=1}^{N} \sum_{i=1}^{n_j} w_k^{i,j} \mathbf{x}_k^i = \sum_{j=1}^{N} X_k^j / C_k \quad (20)$$

$$P_k = \sum_{j=1}^{N} P_k^j / C_k - \hat{\mathbf{x}}_k \hat{\mathbf{x}}_k^{\mathrm{T}} \quad (21)$$

Then estimates and covariances on the HN are transmitted to the sink node at each sample time. Each CN computes local state estimates according to $\hat{\mathbf{x}}_k$ from the HN.

$$p(\mathbf{x}_k \mid \mathbf{z}_{1:k}) \propto \hat{\mathbf{x}}_k \quad (22)$$

(6) Resampling.
If the effective number of particles gets lower than an advance defined threshold, the flag of resampling is set and transmitted to each CN in the cluster. When the set flag is received, the CN performs local resampling via

$$\{\mathbf{x}_k^{i,j}, w_k^{i,j}\} \rightarrow \{x_k^{l,j}, 1/n_j\} \quad (23)$$

However, to maintain the consistency of particles, a global resampling is needed periodically by

$$\{\mathbf{x}_k^{i,j}, w_k^{i,j}\} \rightarrow \left\{x_k^{l,j}, 1/\sum_{j=1}^{N} n_j\right\} \qquad k = sC \quad (24)$$

where *C* is the cycle time of the global resampling and *s* is a positive integer. The particle exchange of the PPF has the same process as the IPF.

5. SIMULATIONS

To test the performance of the IPF and the PPF, they are compared with the IEKF in the tracking accuracy and the CPF in the communication amount. Wireless sensor nodes (N=20) consist of a WSN scene for passive tracking. Each sensor node is modeled as a passive sensor to get bearing observations of the target. Nodes are located randomly between coordinates (0, 0) and (10000, 10000). Initial conditions of tracking are given as follows.

(1) The maximal one-hop communication distance between sensor nodes is r=1000 m, and detection range of the passive sensor is R=3000 m. The sampling period is T=10 s.

(2) The simulated target performs random coordinated turn movement. Original motion parameters of the target are $\boldsymbol{x}_0 = [5000, 8660, 10, 6]$.

(3) Three algorithm based on the PF have the same number of particle M=1000.

(4) Define turn rate sets as [-2, 0, 2] degree/s. The transition probability matrix is selected as

$$P_{ij} = \begin{bmatrix} 0.98 & 0.01 & 0.01 \\ 0.01 & 0.98 & 0.01 \\ 0.01 & 0.01 & 0.98 \end{bmatrix}.$$

In the above simulation scene, the IPF, the PPF, the IEKF and the CPF are used to track the target simultaneously. In [8] range RMSE (root-mean-square errors) of the IPF, the CPF and the IEKF have been analyzed in Fig.2. Tracking trajectories of the IPF, the PPF and the IEKF are compared in Fig.3, and range RMSE are analyzed in Fig.4. Communication amount is counted every 50 s, and the comparison of communication amount is made using the IPF, the PPF and the CPF in Fig.5.

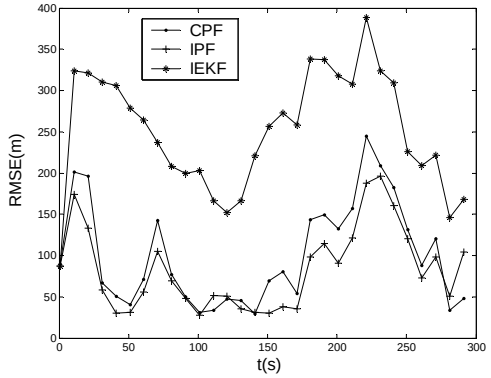


Fig.2. Tracking comparison of IPF, PPF and IEKF

As shown in Fig.2, we have drawn the conclusion that the IPF yielded almost the same accuracy of state estimation as the CPF though the IPF utilized fewer observations than the CPF.

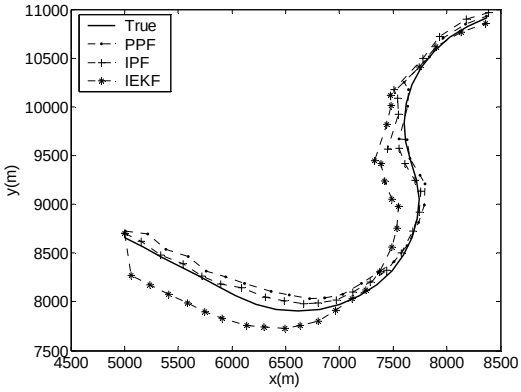


Fig.3. Tracking comparison of IPF, PPF and IEKF

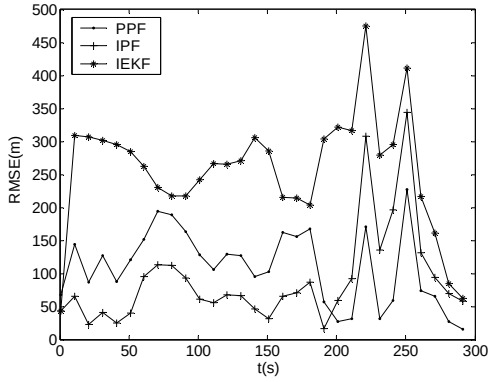


Fig.4. Range RMSE of IPF, PPF and IEKF

Based on above simulations, the following remarks are made.

(1) From Fig.3 and Fig.4, simulation results show that the IPF and the PPF have similar good performance, and that they have higher accuracy than the IEKF in tracking the manoeuvring target.

(2) As shown in Fig.5, the average communication amount in the CPF is proportional to the number of sensor nodes in the scene at each sampling time, so it remains stable during the tracking. Communication amount of the IPF and the PPF varies with the number of nodes in the dynamic cluster.

(3) Although the IPF and the PPF need HN election and state estimate exchange procedure, communication amount of two distributed scheme is 50% less than the CPF during majority tracking processes.

(4) If comparing the IPF with the PPF, we can find that the average communication amount in the IPF is less than the PPF, and that the implementation of the IPF is easier than the PPF, thus the IPF is the best distributed scheme for passive target tracking in WSN.

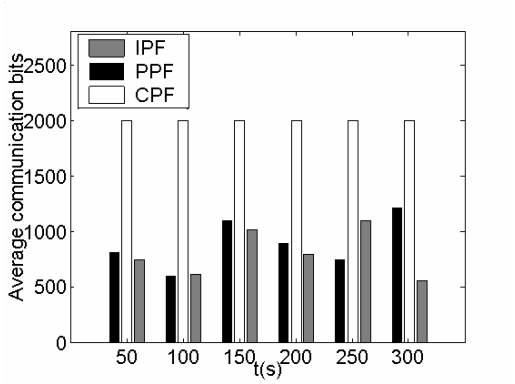


Fig.5. Average communication amount per sample time

6. CONCLUSIONS

In this paper we proposed and compared two distributed particle filter for passive tracking in WSN. Because of the dynamic clustering structure, the distances between HNs and their child nodes are one-hop. Hence multi-hop communication is avoided during the tracking, and communication cost is balanced between sensor nodes. At the same time, two distributed particle filters improve the tracking performance in passive tracking compared with the IEKF. Communication amount of two distributed scheme is less than the CPF, and the IPF has more less communication cost than the PPF for passive target tracking in WSN.

However, these two particle filter schemes still need much energy cost between HNs and their children in updating and resampling, thus future researches should focus on how to reduce communication cost further to realize low-energy distributed tracking in WSN.

REFERENCES

[1] C. Y. Chong and S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," in *Proceedings of the IEEE*, Vol. 91, No. 8, USA: IEEE Press, August 2003, pp. 1247~1256.

[2] N. J. Gordon, D. J. Salmond and A. F. Smith, "Novel Approach to Nonlinear/Non-Gaussian Bayesian State Estimation," *IEE-Proceedings-F*, Vol. 140, No. 2, USA: IEE Press, April 1993, pp. 107~113.

[3] M. Bolic, P. M. Djuric and S. Hong, "Resampling Algorithms and Architectures for Distributed Particle Filters," *IEEE Transactions on Signal Processing*, Vol. 53, No.7, USA: IEEE Press, July 2005, pp. 2442~2450.

[4] V. Teuilere and O. Brun, "Parallelisation of the Particle Filtering Technique and Application to Dopler-bearing Tracking of Maneuvering Sources," *Parallel Computing*, USA: Elsevier Science Press, Vol. 29, 2003, pp. 1069~1090.

[5] Xue Feng, Liu Zhong, and Zhang Xiaorui, "Distributed Particle Filter for Maneuvering Target Passive Tracking," *5th International Conference on Distributed*

Computing and Applications for Business, Engineering and Sciences (DCABES 2006), Hangzhou. Oct 2006, pp. 1196~1198.

[6] M. Efe and D. P. Atherton, "Maneuvering Target Tracking Using Adaptive Turn Rate Models in the Interacting Multiple Model Algorithm," in *Proceedings of the 35th Conference on Decision and Control*, 1996, pp. 51~56.

[7] X. Sheng, Y.-H. Hu and P. Ramanathan. "Distributed Particle Filter with GMM Approximation for Multiple Targets Localization and Tracking in Wireless Sensor Network," *Fourth International Symposium on Information Processing in Sensor Networks*, Los Angeles: 2005, pp. 181~188.

[8] Xue Feng, Liu Zhong, and Zhang Xiaorui, "Decentralized Iinformation Particle Filter for Passive Tracking in Sensor Networks," in *Proceedings of the 1st International Conference on Communications and Networking*, Beijing, 2006, pp. 406/1~406/3.

Feng Xue is a doctor student of System Simulation Lab in Electronics Engineering College, Naval University of Engineering. He was born in 1978, in Liaoning province, China. He received the bachelor's degree and master's degree in weaponry system engineering from Naval Aeronautical Engineering Institute, China, in 1998 and in 2001. He is working in Naval Engineering University, where he works on experimental wireless sensor networks and their application in underwater target tracking and classification.

Design of Embedded EtherNet/IP Gateway and Data Sampling Unit Based on AT91RM9200

Huasong Min, Haiguang Li
College of Computer, Wuhan University of Science and Technology,
Wuhan, Hubei, China
Email: mhuasong@mail.wust.edu.cn

ABSTRACT

Industrial equipment monitoring and control systems are increasingly employing Industrial Ethernet structure. Industrial Ethernet is concerned by many companies and different industrial Ethernet protocols are released, for example, EtherNet/IP, HSE and PROFINET. The EtherNet/IP protocol is a popular industrial Ethernet protocol, which was originally developed by Rockwell Automation and is now managed by the Open DeviceNet Vendors Association (ODVA). It is an already well established industrial Ethernet communication system with good Real-Time capabilities. In the industrial fans monitoring and diagnosis system, an embedded EtherNet/IP gateway and data sampling unit based on 32bit high performance microprocessor AT91RM9200 have been implemented in order to connect Fieldbus with Ethernet. EtherNet/IP protocol stack is realized for the connection between DeviceNet and Ethernet. Besides, ARM Linux and BOA are ported for setting up a web server. User can monitor the status of industrial fans through web browser designed by CGI technique.

Keywords: AT91RM9200, EtherNet/IP, Data Acquisition, BOA, CGI

1. INTRODUCTION

In accordance with the layout of the structure, industrial equipment monitoring and fault diagnosis system has gone through from manual offline monitoring and diagnosis methods, single centralized online monitoring and diagnosis systems, to distributed on-line monitoring and diagnosis systems. The distributed on-line monitoring and diagnosis systems are based on Fieldbus structure. Fieldbus can connect industrial devices and build up devices network easily, but some enterprises adopt different Fieldbus protocols which are incompatible with other enterprises for their own interests, so that devices in different bus network communicate with each other difficultly. On the other hand, enterprises need to connect Fieldbus with office network mostly built on Ethernet protocol, but it is difficult and it needs extra costs. Industrial Ethernet will be a main orientation of the control system network, and it can easily realize the amalgamation between devices network and office network[1].

Industrial Ethernet defines higher layer protocol on the base of Ethernet such as application layer and user layer. It makes use of TCP/IP protocol to transport messages. All in all, it can easily connect with Ethernet, share information, realize integrated management and support remote decision-making. Nowadays, Ethernet is no longer an option for industrial equipment, but it is a requirement in this domain. Ethernet is the fastest growing segment of Industrial Networking for one reason – The Market (Customers) Loves Ethernet. And the most important Industrial Ethernet protocol is EtherNet/IP. EtherNet/IP is an Ethernet solution used in the Rockwell Automation architecture and the one GM is requiring for Robots, Welders and other automation devices[2]. In this paper, the industrial fans monitoring and diagnosis system is taken for example. Its architecture is shown in Fig.1. The embedded EtherNet/IP gateway and data sampling unit is implemented, and is called device unit for short.

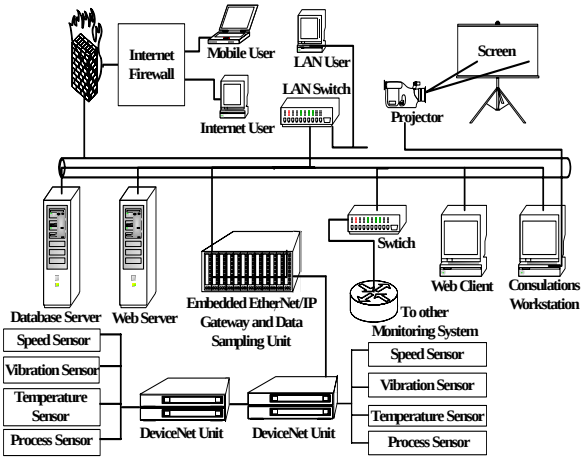


Fig.1. Architecture of the Industrial Fans Monitoring and Diagnosis System

2. HARDWARE/SOFTWARE DESIGN OF THE DEVICE UNIT

2.1 Hardware Architecture Design

Internet communication via TCP/IP protocol is increasingly applied in industrial area. The embedded EtherNet/IP gateway and data sampling unit (device unit) is a solution that enables DeviceNet networks to be coupled together with the Internet/Ethernet, whereby remote monitoring and control is possible. The DeviceNet-Ethernet Gateway controls communication between different networks and makes a transparent DeviceNet-based application interface available to the user. The device unit supports a transparent and protocol-independent transfer of the DeviceNet messages, which allows an implementation into a wide range of possible applications.

The device unit consists of AT91RM9200, CAN controller SJA1000, CAN transceiver PCA82C250 and extended IDE hard disk interface. The AT91RM9200 integrates a lot of standard interfaces including USB 2.0 Full Speed Host and Device, Ethernet 10/100 Base-T Media Access Controller (MAC), which provides connection to an extensive range of external peripheral devices and a widely used network layer. The AT91RM9200 EMAC connects with Ethernet through DM9161E, which is an Ethernet physical layer transceiver offered by DAVICOM. The AT91RM9200 connects with CAN controller through SPI interface[3].

The AT91RM9200 embeds a Compact Flash Glue Logic that can be adapted to support a peripheral IDE hard disk. The

External Bus Interface (EBI) integrates circuitry to interface with Compact Flash devices using Attribute, Memory and I/O modes. Most of these signals can be used to connect a hard disk drive to the AT91RM9200. The EBI Compact Flash Glue Logic integrates a fourth memory space that can be accessed through NCS4. This memory space, True IDE Mode Space, is intended to access Compact Flash in True IDE Mode. Hardware architecture of the device unit is presented in Fig.2.

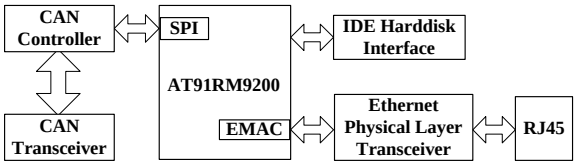


Fig.2. Hardware Architecture of the Device Unit

2.2 Software Architecture Design

Software architecture of the device unit consists of bootloader, ARM Linux, CAN device driver, EtherNet/IP protocol stack, Gateway routing program, massive data acquisition and store program, TCP/IP protocol stack, BOA web server and CGI web program. They locate in different layers. Lower layer supply services for higher layer. Software architecture of device unit is presented in Fig.3.

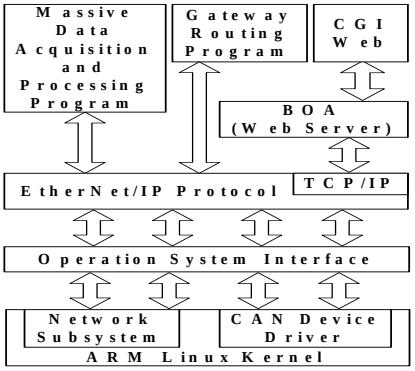


Fig.3. Software Architecture of the Device Unit

1) Bootloader
   Bootloader initializes the kernel hardware. It copies operation system kernel to RAM from flash memory, and executes the kernel. On the other hand, it provides interface to send commands to device unit or to inform user the state of device unit. Porting u-boot can boot up the device unit hardware for loading operation system. U-boot is developed by Wolfgang Denk. It supports several architectures such as MIPS, PPC, ARM and X86. Its source code can be downloaded from http://sourceforge.net.
2) ARM Linux
   ARM Linux is a successful example of porting the Linux Kernel to ARM processor, led mainly by Russell King. It is under almost constant development by various researchers and organizations around the world. The ARM Linux kernel is being ported, or has been ported to more than 500 different machine variations, including complete computers, network computers, hand held devices and evaluation boards. ARM Linux operation system is ported to the device unit to manage the hardware and support virtual machine.
3) EtherNet/IP protocol stack
   EtherNet/IP encapsulates CIP messages and transports them on Ethernet by TCP/IP protocol. All encapsulation messages, sent via TCP or sent to UDP port 0xAF12, are composed of a fixed-length header of 24 bytes followed by an optional data portion. The total encapsulation message length shall be limited in 65535 bytes.
4) BOA web server
   In the embedded system, three type web servers can be ported: httpd, thttpd, and BOA. The BOA web server is a light weight nearly full featured web server. It has cgi-bin and authentication support. It is also a single tasking - not spawning of multiple processes to handle simultaneous requests. BOA's memory footprint is extremely small (about 85k when running).
5) CGI web program
   CGI can be programmed by embedded C code, or be embedded with html script. Firstly, the remote web Client send request through URL to CGI. Then, the CGI execute it to get the buffered information of devices which belong to lower DeviceNet network. Finally, the web page with result (include the information of industry devices) will be back to the remote web Client.

3. IMPLEMENTATION OF THE DEVICE UNIT

3.1 Port EtherNet/IP

EtherNet/IP is a communication system suitable for use in industrial environments. EtherNet/IP allows industrial devices to exchange time-critical application information. EtherNet/IP uses CIP (Control and Information Protocol).The common network, transport and application layers also are shared by ControlNet and DeviceNet. EtherNet/IP makes use of the standard Ethernet and TCP/IP technology to transport CIP communication packets. The result is that a common open application layer is on the top of highly popular Ethernet and TCP/IP protocols[4]. EtherNet/IP protocol stack is presented in Fig.4.

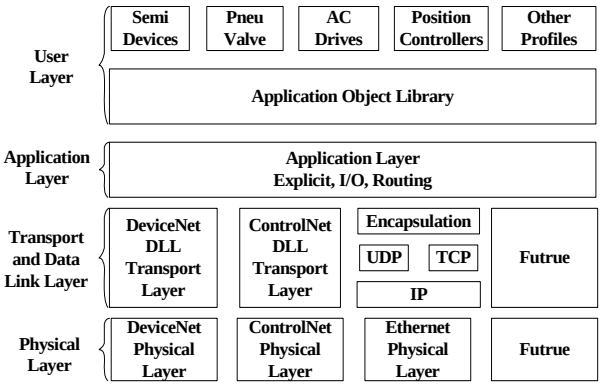


Fig.4. EtherNet/IP Protocol Stack

The EtherNet/IP example code can be downloaded from www.odva.org freely. The example code stack is written in order that direct operating system calls are isolated within generic operating environment functions and #defines. The organization of the OE services has been designed to simplify the porting of the example code to different multitasking

kernels and hardware platforms. The following operating environment files of the example code need to be modified as follows to support the ARM Linux operating system[5].

1) OE.H
   This file is provided to specify a common and consistent operating environment interface definition. The interface definitions in the file are external functions defined in ARM Linux kernel. Function prototypes given here are used. For example, OE_CreateSemaphore() means dynamically creating a semaphore at run-time.
2) OE_LSERV.H
   This file contains all the redefinitions of the standard OE services to match the local operating system. To port the Example Code to ARM Linux environment, redefinitions of the standard OE services are supplied to adapt to definition of ARM Linux kernel. For example, OE_CreateSemaphore() is redefined as CreateSemaphore().
3) OE_LTYPE.H
   This file contains the local redefinitions of data types specified in the public interfaces of the operating environment example code that need to match the local operating system. For example, OE_SemaphoreType is redefined as UL (unsigned long).

3.2 EtherNet/IP Gateway Routing Program

When the gateway receiving CIP messages from EtherNet/IP network, it judges whether users locate in the local network or remote DeviceNet network. If users locate in the local network, the gateway will shield the CIP messages. Otherwise, the gateway will repackage the messages and transmit them to DeviceNet. Similarly, when receiving CIP messages from remote DeviceNet network, the gateway judges whether users locate in the local network by id of users. If users locate in local DeviceNet network, the gateway will shield the messages. Otherwise, the gateway will encapsulates the CIP messages into TCP (UDP) /IP messages and transmit them to EtherNet/IP network. All these process are presented in Fig.5.

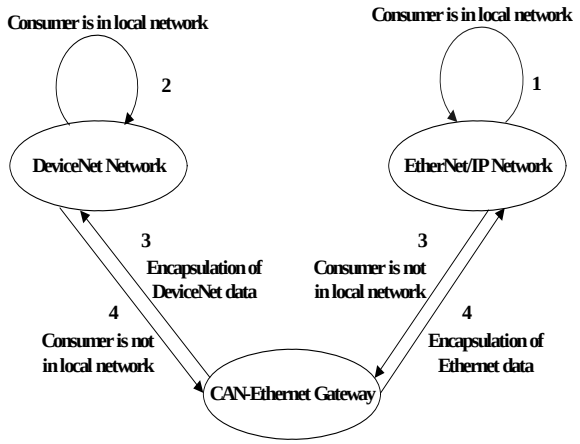


Fig.5. EtherNet/IP Gateway Routing

3.3 Massive Data Acquisition and Store Program

The massive data acquisition program should be running on the EtherNet/IP gateway. It is implemented by Visual C++ 6.0 program Tool. Its function include data acquisition when the fan is normally running in the system, sampling data acquisition and the forming of alarm hint information and history data. The system needs a few data information for further use such as basic parameters of the device, real-time data, history data, the threshold value and sampling data. The basic parameters of the device contain basic parameter of channels, sampling frequency and alarm value. The real-time data is continuously gotten by data acquisition program, and they stand for device status information. The history data is gotten after time averaging the original real-time data. The threshold value is mainly swing value of the vibration event. The sampling data is higher frequency data when vibration event occurs using for fault diagnosis and signal analysis.

Besides sampling data, all other data information can store into the designed database. As the quantity of acquisition data is very large, and it is accumulated day by day, it is not appropriate to store them into database. In the system, sampling data is stored into the IDE hard disk that is specially extended. The adopted format of stored data is text format, which is convenient for reading data from the IDE hard disk when the fault diagnosis system is working.

The whole process is mainly described as follows: First, data acquisition parameters should be initialized, and each state eigenvector is set to a lower sampling frequency. Then, data of lower frequency are processed. A certain number of data can be transformed in memory using FFT method. The transformed data will be compared with the threshold value. If it is less than the threshold value, there are two processing ways to the transformed data. One is storing them into the original real time database for on-line supervision. The other is that an average of them in certain time should be stored into the history database. If it exceeds the threshold value, a sampling of lower frequency shall be terminated. At the same time, a sampling event of higher frequency must be triggered. Higher frequency data could be stored into the IDE hard disk, and the sampling event of higher frequency is written into sampling database. All these process are presented in Fig.6.

3.4 Port BOA

First, BOA source code can be downloaded from http://www.boa.org. Then, cross compile tool chain cross-2.95.tar.bz2 need to be downloaded from ftp://ftp.arm.linux.org.uk /pub/linux/arm/toolchain because the downloaded BOA is used on AT91RM9200.

Before compiling the BOA source code, some configuration need done.

1) Compile BOA to kernel
   In order to compile BOA into Linux kernel, the following command must be executed:
   make menuconfig
   In the application selection menu, choose BOA under the Network Application Volume.
2) Rewrite boa.conf file
   Under the ARM Linux Operation system, the allocation of user application usually is provided by configuration files. The content of boa.conf file is rewritten as follows. They indicate http homepage location contents.
   ServerName AT91RM9200
   DocumentRoot/home/httpd
   ScriptAlias/cgi-bin/home/httpd/cgi-bin/
   ScriptAlias/index.html/home/httpd/index.html

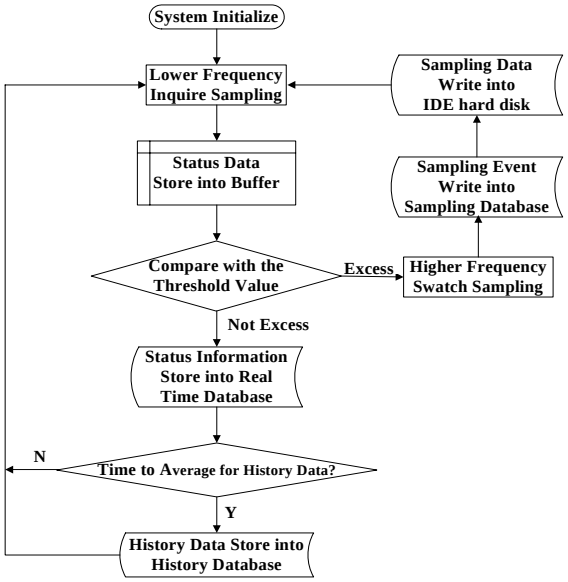


Fig.6. Flowchart of data acquisition and store program

3) Rewrite BOA makefile

In BOA makefile, change cc gcc to arm-Linux-gcc and change cpp gcc –E to arm-linux-g++ -E for the necessity of compiling ARM target binary code.

After above steps, the final binary code can be downloaded into the device unit.

3.5 CGI Web Design

The CGI program is written by c code, and usually compiled together with the source code of ARM Linux and BOA. The CGI binary code is put under /home/httpd/cgi-bin volume. The CGI programs can use GET, POST or Direct URL Parameter Passing method to communicate with remote web Client.

Users can view the real-time information (actually it is buffered by EtherNet/IP gateway data sampling process) of industrial devices on the remote office computer[7]. A fan vibration remote monitor page on the device unit is realized. The example web page is presented in Fig.7. If an active, real-time self-refreshing page is requested, a little flash program or java Applet on PC can be designed, which is put the file together with embedded html file. Because the flash and java applet program are executed on web Client PC after downloading web Client from the device unit, the program can be only compiled for PC running, not for ARM board, using TCP sockets technology to communicate.

4. CONCLUSIONS

Compared with the existing Fieldbus, industrial Ethernet is more powerful, open, and conveniently integrated with the control system. Now it will come to industrial Ethernet times. DeviceNet and Ethernet can be relaxed to achieve sampling interconnection by porting industrial Ethernet protocol EtherNet/IP to the embedded EtherNet/IP gateway and data

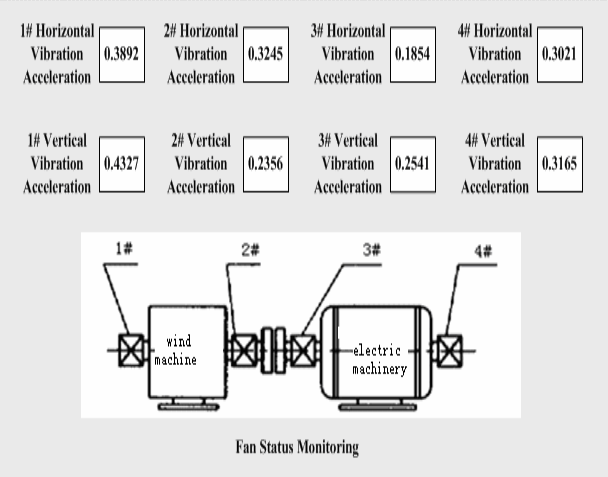


Fig.7. Example Web Page

unit. At the same time, the existing DeviceNet structure does not need to be amended, so the integration between Fieldbus control network and office information network can be easily achieved, and the remote monitoring and decision system is also supported.

The embedded EtherNet/IP gateway and data sampling unit in the industrial fans monitoring and diagnosis system has the following three advanced features. A). Compatible with industrial Ethernet protocol, can communicate with EtherNet/IP devices and Fieldbus devices on-line. B). Support monitoring industrial fans status through web browser. C). Support high-capacity data storage, a state of the black box monitoring equipment for accident information recourse.

REFERENCES

[1] ControlNet International and Open DeviceNet Vendor Association, EtherNet/IP Specification[R], Jun 5, 2001.

[2] ODVA, Networks Build on a Common Industrial Protocol [R], http://www.odva.org.

[3] ATMEL ARM920TTM-based Microcontroller AT91RM 9200 User's Manual[R],Aug 2003.

[4] Rinaldi, John, “EtherNet/IP-An application layer protocol for industrial automation[J],” *Sensors (Peterborough, NH)*, May, 2003, vol 20, No 5, pp.43-45.

[5] Gu Deying, He Fenghang, “Realization of EtherNet/IP Protocol on Linux [J],” *Chinese Journal of Scientific Instrument* , 2005, Vol.26, No.z2, pp. 441-444.

[6] BROOKS P. EtherNet/IP - industrial protocol [A], Antibes - Juan Les,Jan 2001, pp.505 – 514.

[7] Igor Klimchynski, “Extensible Embedded Web Server Architecture for Internet-Based Data Acquisition and Control[J],” *IEEE Sensors Journal*, 2006, vol.6, No.3, pp.804-811.

Huasong Min is an associate professor and a head of embedded system real-time software lab, dean of Computer Science and Technology College, Wuhan University of Science and Technology. He is a committeeman of embedded system expert committee in China Electronic Institute. He got a doctor degree from Wuhan University in 2006. His research is focused on embedded system and PSoC(Programmable System-On-Chip) technology, VOIP/SIP multimedia communications, and network remote fault diagnosis based on AOP(Agent Oriented Programming).

Haiguang Li is a master with specialty of computer application in Computer Science and Technology College, Wuhan University of Science and Technology. He graduated from Wuhan University of Science and Technology in 2005. His graduated paper got the first prize of excellent papers in Hubei province.

An Admission Control Agorithm for Ad Hoc Networks*

Sihai Zheng, Layuan Li
School of Computer Science and Technology, Wuhan University of Technology
Wuhan, Hubei , China
Email: zhen672@sohu.com

ABSTRACT

The study of admission control in mobile Ad Hoc networks is attracting more attention recently. Ad Hoc networks are unpredictable by nature. Providing any kind of reliability for Quality of Service(QoS) in such networks is challenging. Based on traditional Admission Control algorithm, the authors had improved Adaptive Admission Control(AAC) algorithm for Ad Hoc networks. Improved AAC can provide precise resource estimation and quality prediction for admission decisions, considering inherent wireless multihop communication characteristics, carrier sensing and mobility. At last, this paper realized it successfully with AODV protocol in NS 2. According to the result of simulation, the anticipated outcome has been achieved.

Keywords: Ad Hoc, QoS, AODV, Admission Control

1. INTRODUCTION

Multimedia applications are very popular in fixed networks. The ability to run such real-time application over mobile ad hoc networks is very attracting .Unfortunately, most of the routing protocols only provide best-effort service[1] which is not suitable for multimedia applications in ad hoc networks.

Ad hoc network nodes operate in a very volatile environment where any connection could be dropped at any moment. Consequently, providing QoS in wireless mobile ad hoc networks should be addressed differently. A strategy is required to ensure predetermined service performance constraints in ad hoc networks. This strategy consists of evaluating, finding, and managing resources for different QoS requiring communication flows.

This paper had improved the CSMA based adaptive admission control(AAC) algorithm[2] which is presented by R.de Renesse. Improved AAC algorithm aims to provide precise resource estimation for admission decisions, considering inherent wireless multihop communication characteristics, carrier sensing and mobility. It ensures that any QoS flow is transmitted at the requested rate with minimum end-to-end delay, by managing the bandwidth efficiently. When QoS guarantees can no longer be provided, due to network mobility or congestion, Improved AAC informs preselected traffic sources and pauses their transmission. Thus wastage of resources is avoided and the requested QoS of other on-going sessions is respected. At last, the authors realized improved AAC algorithm successfully with AODV in NS 2.

2. IMPROVED AAC ALGORITHM

CSMA(carrier sensing multiple access) protocols are widely used in wireless communication networks. These protocols use carrier sensing, and handshake techniques to reduce collision probability, due to the *hidden node* and the *exposed node* problem. In this environment, each transmitted flow uses resources that are shared between nodes within the carrier sensing range. Generally, the carrier sensing range is twice the size of the transmitting range[3]. Therefore, the transmission impacts on nodes beyond the transmitting range. Furthermore, when the transmission is done over multiple hops, interferences created by the traffic becomes much greater. If nodes' sensing range overlap at a maximum of *n* times over one of the intermediate nodes, this node's available bandwidth decreases by a factor of *n* times the rate of the traffic. Therefore, another strategy is needed to precisely predict at each node, how much bandwidth is necessary for a specific traffic rate. This effect is called *intra-flow contention*[4].

Admission control[5] is used to assist the routing protocol in its search for the best QoS routes. A call for transmission is admitted only if there exists a path with enough available resources to carry a flow, with specific service performance constraints.

2.1 Estimation of Available Resources

The bandwidth is the most important factor for QoS guarantees. How to estimate the available bandwidth is the key of improved AAC algorithm.

2.1.1 Average Bandwidth Calculation

The average used bandwidth over the period of time *T* is[2]:

$$BW(bps) = \frac{N \times S \times 8}{T} \qquad (1)$$

N is the number of packets sent and received by a node over a period of time *T*; *S* is the size of these packets in bytes. We assume that *S* is known.

The accuracy of the bandwidth calculation depends on the interval *T*, between consecutive measurements. The larger *T* is ,the more accurate the results are. However, *T* must be small enough to be transparent to the channel dynamics.

2.1.2 Available Bandwidth Acquirement

Assume two nodes are within transmission range of each other. The available bandwidth on the link between these two nodes, is the minimum of the available bandwidth of all nodes, belonging to their sensing range. Improved AAC algorithm uses HELLO messages in order to acquire the available bandwidth of the 1-hop neighbours only. Therefore, Each node sends classic HELLO messages with one extension: *Available Bandwidth*. This corresponds to the available bandwidth of the source node sending HELLO message. Each node receiving this HELLO message, stores the *Available Bandwidth* value in the cache table. If the available bandwidth of current node is less than its 1-hop neighbours', it would propagate RREQ and RREP message. Else it would drop RREQ/RREP message.

2.2 QoS Route Discovery

*Support by: Nature science foundation of China (No.60672137) and Specialized Research Fund for the Doctoral Program of Higher Education (No. 2006497015)

Improved AAC algorithm uses AODV[6] for routing. Before a source node sends traffic, a RREQ message is broadcasted into the network. Each intermediate node broadcasting the RREQ creates a backward pointer towards the source. When the destination receives the route request, it initiates a RREP message that is delivered to the source node using the backward pointer. Thus, a path has been found between the source and the destination and the traffic is allowed to start.

A node's interference range is more than twice the size of its transmission range. In other words, the available bandwidth changes of a node interfere with nodes within the 2-hop range. In order to provide a good estimation of the expected intra-flow contention, the *Contention Count* has to be calculated, using the *Hop Count* field of the RREQ/RREP packets.

During RREQ/RREP query cycle, The RREQ gives the number of hops between the source node and the current node, whereas, the RREP gives us the number of hops between the destination node and the current node. Let's call h_{req} and h_{rep} the number of hops respectively given by the RREQ and RREP. *Contention Count*(*CC*) is defined as the following[2,4]:

$$CC = W_{req} + W_{rep} + W_{curr} + W_{dest} \quad (2)$$

W_{req} and W_{rep} correspond respectively to the weight of upstream and downstream nodes in terms of interference. W_{curr} is the weight of the current node transmissions, relative to the traffic. Finally, W_{dest} is the weight of the destination node.
Every node on the path interferes with, at most, two upstream and downstream node, therefore:

$$\begin{cases} h_{req} \geq 2 \Rightarrow W_{req} = 2 \quad else \quad W_{req} = h_{req} \\ h_{rep} \geq 2 \Rightarrow W_{rep} = 2 \quad else \quad W_{rep} = h_{rep} \end{cases} \quad (3)$$

W_{curr} always equals 1 because the current node transmit the traffic only once. Therefore:

$$\forall h_{req}, \ \forall h_{rep} \quad \Rightarrow \quad W_{curr} = 1 \quad (4)$$

The destination node interference weight depends on the type of communication used. Here, we assume unidirectional communication. If the destination node is within the current node's sensing range, an interference weight of 1 is included in W_{rep}. This weight has to be subtracted, hence:

$$h_{rep} \geq 3 \Rightarrow W_{dest} = 0 \quad else \quad W_{dest} = -1 \quad (5)$$

The *CC* definition given by equation（2）can be simplified as follows:

$$\begin{cases} if \quad h_{req} > 2 \quad \Rightarrow \quad h_{req} = 2 \\ if \quad h_{rep} > 3 \quad \Rightarrow \quad h_{rep} = 3 \\ CC = h_{req} + h_{rep} \end{cases} \quad (6)$$

An example is shown on Figure 1. At the current, h_{req}=3 and h_{rep}=4.Here, $h_{req}>2$, $h_{rep}>3$, therefore, if we apply equation (6), h_{req}=2， h_{rep}=3， $CC = h_{req} + h_{rep}$=5.

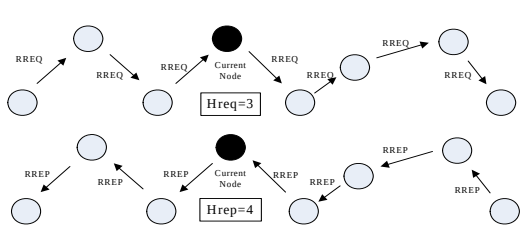


Fig. 1. Number of Hops Given by RREQ/RREP

As we need both h_{req} and h_{rep}, the calculation can be done only after the RREP is received. Then, one checks if the available bandwidth is large enough to accept a drop of $CC \times Rate$. If the check is true, the RREP message is forwarded to the source. With this technique, a bandwidth reliable path is set up and quality of service is guaranteed.

2.3 Maximum Rate Allowance Scheme

Since *CC* values are different for each node on the traffic route, the amount of predicted interference that would be created by the traffic can be maximized. If the traffic rate combined with its maximum *CC* is greater than the available bandwidth, the session is rejected. Thus, a *maximum rate allowance scheme* can be established, depending on the maximum *CC* value on the path.

Let's call *R* the rate of the traffic, *CC(i)* the contention count at node *i*, and, MAC_{ovh} the Medium Access Control overhead in %.the corresponding used bandwidth at this node is:

$$BW(i) = CC(i) \times R \times (1 + MAC_{ovh}) \quad (7)$$

Hence, the maximum bandwidth used on the route between source and destination is :

$$BW_{\max} = \max_{\forall i}(CC(i) \times R \times (1 + MAC_{ovh})) \quad (8)$$

The maximum bandwidth that we can use is limited to BW_{lim}. Therefore, one can derive the maximum rate which will be allowed by the protocol, depending on the maximum *CC* on the path, thus:

$$R_{\max} = \frac{BW_{\lim}}{(1 + MAC_{ovh}) \times CC_{\max}} \quad (9)$$

A QoS flow could be admitted by AAC when the values of traffic rates is less than R_{max}, else it would be rejected. The maximum allowed traffic rate decreases exponentially, along with the number of hops in the path .Therefore, the shorter a path is in terms of the number of hops ,the higher the achievable bandwidth.

2.4 QoS Flow Management

Compared to AODV, improved AAC added several extensions to the routing tables and RREQ/RREP messages in order to provide QoS.

Since AAC focused only on bandwidth requirements, we have added two extensions to the Route Request and Route Reply packets, which are the *session identity number*, and the *requested session rate*. we use the term session rate instead of minimum bandwidth, because we want improved AAC to perform call admission according to the traffic source information. For a specific session rate, the bandwidth utilization may vary depending on lower layer standards. Each node determines whether it has enough resources to carry the traffic, based on these extensions.

If there is not enough available bandwidth for the traffic, the node simply drops respective RREQs/RREPs. RREQs/RREPs passing through the network fulfilling this condition set up QoS routes. The session characteristics are stored in the routing table of each node belonging to the route, during the RREP propagation, if there is still enough available resources. For each routing entry, we also added a field containing a list of s*ession objects*[7]. Each s*ession object* is composed of a *session identity number*, a corresponding *session rate*, and the *source identity* of this session.

All active nodes keep a list of all source nodes whose traffic passes through them, along with the requested levels of QoS. Therefore, if an active node notices that its available bandwidth drops significantly under a specified limit, it initiates a *QoS LOST* packet, containing the address of the destination and the

session id of the flow. This packet is sent to the corresponding source node. When the source node receives the *QoS LOST* packet, it looks at the destination address contained in the packet, finds the corresponding entry in the routing table, declares the route in *QoS Repair*, pauses the traffic, and initiates a new route request for the destination node.

3. ALGORITHM REALIZATION

We had modified AODV protocol to realize improved AAC algorithm in NS2. Several extensions had been added to the routing tables and RREQ/RREP messages. The decision on whether to accept a transmission request for a new QoS flow, is based on the information provided by the extensions.

3.1 Routing Table Extension

The following list had to been added to each routing entry:
(1) Session Identity;
(2) Session Rate;
(3) Source Identity;
(4) Maximum Delay;
(5) Minimum Available Bandwidth;
(6) List of Sources Requesting Delay Guarantees;
(7) List of Source Requesting Bandwidth Guarantees.

3.2 RREQ Extension

A node appends a *QoS Object* extension[8] to a RREQ in order to discover a path that satisfies the QoS parameters which are present in the *QoS Objec*t, which is situated within the *QoS Object* extension data. Fig 2 shows *QoS Object* extension format.

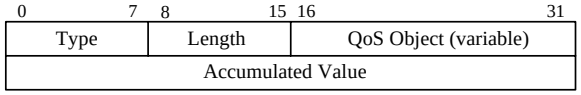


Fig. 2. QoS Object Extension Format

When a node initiates a RREQ message, it may append a *QoS Object* extension after the RREQ data, optionally followed by *Accumulated Value* extensions according to the specific data in the *QoS Object* extension. *Accumulated Value* provides information about the cumulative value that has been experienced by nodes along the path from the source node to the node currently processing the RREQ. The *Accumulated Value* extension must be appended to a RREQ by a node rebroadcasting a request for a QoS route whenever it is needed to measure the accumulated value of the parameter of the type given in the *QoS Object* field. This allows each next intermediate node, or the destination, to determine whether the path can still meet the required parameter specification within the *QoS Object* data.

3.3 QoS Routing Operation

Figure 3 is the flow chart of Qos routing discovery and maintenance.

3.4 Protocol Modification

AODV protocol in NS 2 had been modified to realize improved AAC algorithm. The main files that were modified were listed as following[9].

(1) ns\aodv\aodv.cc, aodv_rtable.cc, aodv.h, aodv_pachet.h, aodv_rtable.h;
(2) ns\mac\channel.cc, channel.h;
(3) ns\tools\cbr_traffic.cc, cbr_traffic.h;
(4) ns\trace\cmu-trace.cc, cmu-trace.h.

Protocol was named as AAC-AODV when the modification were completed.

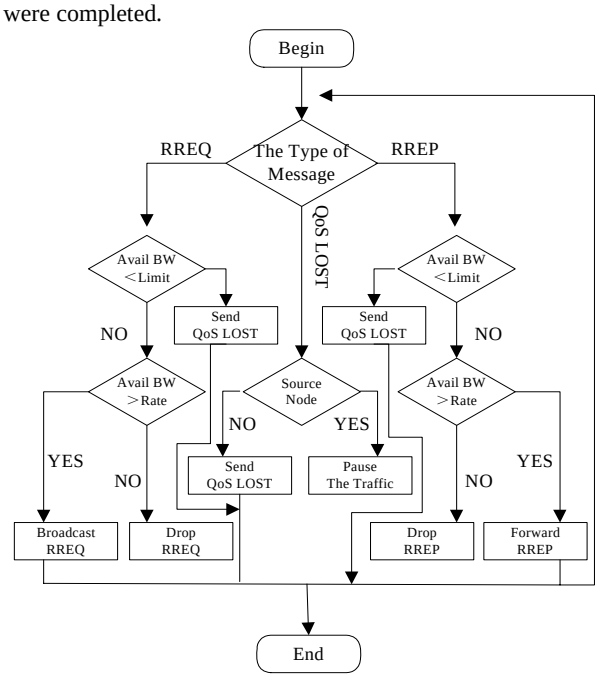


Fig. 3. Flow Chart of QoS Routing

4. PERFORMANCE EVALUATION

Simulations have been done using ns version 2.27 under Linux. The scenario consists of 30 nodes moving in a 500m×500m topology. We chose the *Random Waypoint Model* provided by ns-2, as the mobility model. The traffic models were generated for 30 nodes with cbr traffic sources, with maximum connections of 10 at a rate of 100kbps. We use the IEEE 802.11b MAC protocol. The channel data rate is set to 11 Mbps. The MAC overhead is set to 45%, the bandwidth interval *T* from 0.8 to 0.4 seconds, and packets size to 1024 bytes. The simulation time is 100secs. QoS-AODV[5] and AAC-AODV are used as routing protocols.

4.1 Performance Metrics

Three important performance metrics are evaluated[10]:
(1) Packet delivery fraction － the ratio of the data packets delivered to the destinations to those generated by the CBR sources.
(2) Average end-to-end delay of data packets－This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.
(3) Normalized routing load－The number of routing packets transmitted per data packet delivered at the destination.

4.2 Performance Comparison

Fig 4 plots the *Packet delivery fraction*. The packets deliver rate of AAC-AODV is higher than QoS-AODV obviously. It show that improved AAC algorithm can increase effectually packet delivery rate.

Fig 5 plots the *Average end-to-end delay* of data packets. One notices that the delay values of QoS-AODV is much higher. QoS-AODV's bad delay performances is normal since no admission control is performed, thus leaving nodes under saturation.

Finally, the *Normalized routing load* results are shown on Figure 6. AAC-AODV involve low routing load. QoS flow are rejected by admission control when there are not sufficient QoS guarantees. Thus some unnecessary route messages are avoided, routing load was reduced.

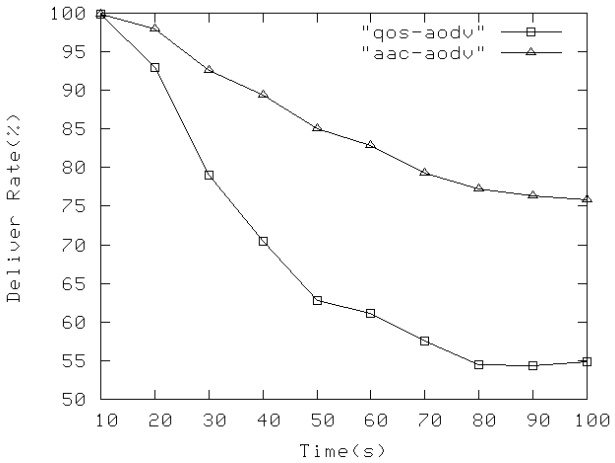


Fig. 4. Packet Delivery Fraction

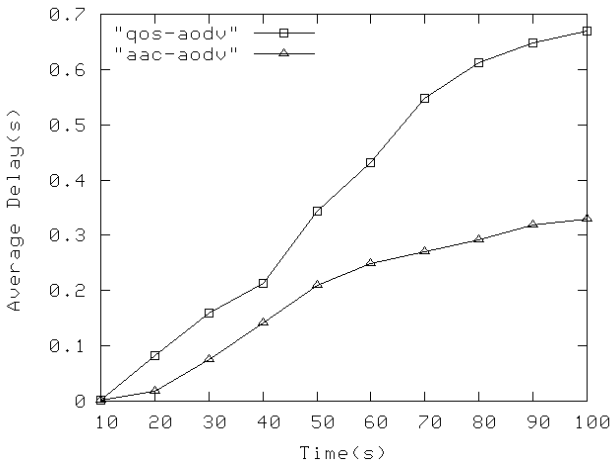


Fig. 5. Average End-to-End Delay

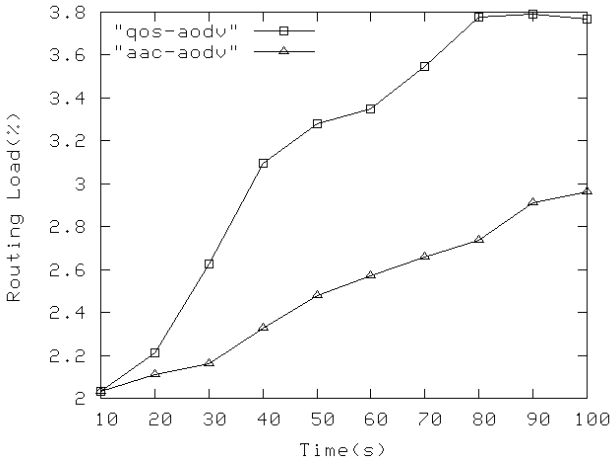


Fig. 6. Normalized Routing Load

5. CONCLUSION AND FUTURE WORK

We demonstrated, through simulation evaluation, that improved AAC algorithm provides reliable QoS guarantees. It uses an exclusive combination of strategies which considers intra-flow contention, mobility and carrier sensing, along with minimizing complexity and control overhead.

We are currently focusing on adapting AAC algorithm for other on demand routing protocol(such as DSR and TORA). The main aim of our future research is to provide efficient QoS routing protocols for ad hoc networks.

REFERENCES

[1] Huang C. Dai F. Wu J, “On-Demeand location-aided QoS routing in Ad Hoc networks”, In: *Proc. of the Int. Conf. on Parallel Processing (ICPP),*2004, pp.502~509.

[2] R. de Renesse, M. Ghassemian, V. Friderikos, A.H. Aghvami, “Adaptive Admission Control for Ad Hoc and Sensor Networks Providing Quality of Service”, *Technical Report*, UK, May 2005, pp.6~12.

[3] I. Joe, “Reservation CSMA/CA for QoS Support in Mobile Ad Hoc Networks”, Lecture Notes in *Computer Science*, Vol.3842, pp.231-235, Jan 2006.

[4] Y. Yang, R. Kravets, “Contention-Aware Admission Control for Ad Hoc Networks”, Univ. Illinois at Urbana-Champaign, Urbana-Champaign, IL, Tech. Rep. 2003-2337, 2003.

[5] Ronan de Renesse, Mona Ghassemian, Vasilis Friderikos, “A. Hamid Aghvami. QoS Enabled Routing in Mobile Ad Hoc Networks”,*Technical Report*, UK, May 2005, pp.2~14.

[6] Perkins C, Belding-Royer E, Das S, “Ad Hoc on-demand distance vector (AODV) routing”, *Request for Comment (RFC)*: 3561,2004.

[7] Li Layuan,Li Chunlin, “A hierarchical QoS multicast routing protocol for mobile ad-hoc networks”, *Chinese Journal of Electronics*,2006,15(4), pp.573~577.

[8] Sun Baolin, Li Layuan, Hua Chen, “An entropy-based model to support QoS multicast routing optimization algorithm for mobile ad hoc networks”,In:*Proc. IEEE WCNM*, pp 73~738, sep 2005.

[9] Lap Kong Law,”NS-2 Tutorial. Dependable Computing Lab”,2003, pp.1~20.

[10] “The Network Simulator ns-2”, http://www.isi.edu/nsnam/.June 2007.

Sihai Zheng, was born in Hubei, China on 28 October 1975. He is master candidate of computer science and Technology of Wuhan University of Technology. He graduated from Hubei Institute for Nationalities in 1999 with specialty of computer networks. His research interests include computer networks and protocol engineering.

Layuan Li, was born in Hubei, China on 26 February 1946. He received the BE degree in Communication Engineering from Harbin Institute of Military Engineering, China in 1970 and the ME degree in Communication and Electrical System from Huazhong University of Science and Technology, China in 1982. He academically visited Massachusetts Institute of Technology(MIT), USA in 1985 and 1999, respectively. Since 1982,he has been with the Wuhan University of Technology (WUT), China, where he is

currently a professor and Ph.D tutor of Computer Science, and editor in chief of the Journal of WUT. He is Director of International Society of High-Technol and paper reviewer of several IEEE Transactions and Jounals. He was the head of the Technical Group of Shaanxi Lonan PO Box 72, Ministry of Electrical Industry, China from 1970 to 1978. His research interests include computer networks, protocol engineering and image processing. Professor Li has published over one hundred and fifty technical papers and is the author of six books. He also was awarded the National Special Prize by the Chinese Government in 1993.

Interconnecting IPv4/IPv6 Metwork in Pure IPv6 Backbones with Extended IPv4-over-IPv6 Mechanism

Jian Song[1], Mian Huang[2], Wei Sun[1], Yu Jiao[3], Baojie Zhang[4]
[1]The college of Network Education, LanZhou University of technology, Gansu, LanZhou, 730050
[2]The school of Computer and communication, Lanzhou University of technology, Gansu, Lanzhou, 730050,
[3]Architectural Engineering College, He Nan University of science and technology, Henan, Luoyang,471003
[4]Staff Room of Wireless Communication, Xi'an Institute for Communication, Shanxi, X i'an, 710106)
Email:net-cn@163.Com

ABSTRACT

With the development of the IPv6 technology, native IPv6 backbones are emerging. It's a hotspot of researches in this stage that IPv4 networks interconnect over IPv6 backbones. IPv4-over-IPv6 mechanism is regarded as a good scheme for it. However, with the IPv6 networks deploying, IPv4-over-IPv6 mechanism has several limitations. In this paper, we analyzed the limitations, and proposed a new kind of IPv4-over-IPv6 extended mechanism. The new mechanism not only inherits advantages of the IPv4-over-IPv6 mechanism, but also solves the problem that IPv4 applications in the IPv6 nodes can not communicate with the IPv4 nodes.

Keywords: IPv4-over-IPv6, Transition, Interconnection Between IPv4 and IPv6

1. INTRODUCTION

With the development of the IPv6 technology, native IPv6 backbones (such as CNGI) are emerging. However, vast applications and services still stay in IPv4 network. Interconnection of IPv4 and IPv6 networks over pure IPv6 backbones is required. On the 13th annual meeting of CERNET in Nov. 2006, Mr. Ma-Yan, Professor of BUPT, presented the deployment of IPv4-over-IPv6[1] [2] on CNGI-CERNET2. It is regarded as a good way for the interconnection of vast IPv4 networks through pure IPv6 backbone, and first developed by the Network Protocol Test laboratory of Tsinghua University. In Nov. 2005, Tsinghua University and the International research lab paid attention to this mechanism and made a RFC draft[3] in Sep. 2006.The idea of this mechanism is as follows: nodes in the IPv4 domain of IPv4-over-IPv6 is still communicated by IPv4 protocol. When IPv4 packets across the IPv4-over-IPv6 edge router from the IPv4-over-IPv6 intra-domain, the edge router transforms these IPv4 packets into pseudo IPv6 packets, and across the IPv6 backbone to reach the end IPv4-over-IPv6 edge router. Then the pseudo IPv6 packets arrive at IPv4-over-IPv6 edge router from the IPv6 backbone, the packets will be transformed into IPv4 packets, and routed to the end node by IPv4 routing protocol.

Most importantly, the IPv4-over-IPv6 mechanism doesn't need to upgrade the existing software because that the software of IPv4-over-IPv6 intra-domain nodes is still worked under IPv4 protocol. It can fully perform the function of generating IPv4 networks through pure IPv6 backbone.

However, the IPv4-over-IPv6 mechanism only meets the needs of the interconnection between IPv4 networks via the IPv6 backbone. It is useless to interconnect the IPv4 nodes and pure IPv6 networks (the communication using IPv6 protocol only in the network) through this mechanism. The detailed analysis is in section 3.2 of this paper.

In this paper, an extended mechanism of IPv4-over-IPv6 method is proposed in order to solve the above problems. This mechanism inherits the merit of IPv4-over-IPv6 method and realizes the transparent communication of nodes in pure IPv6 network and IPv4.

2. THE IPV4-OVER-IPV6 MECHANISM

2.1 The principle of IPv4-over-IPv6 mechanism

IPv4-over-IPv6 mechanism is shown in Fig.1.

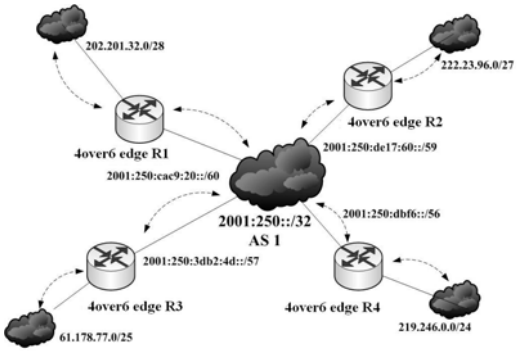


Fig.1. Principle of Ipv4-over-Ipv6 mechanism

R1, R2, R3, R4 are edge routers. Through the IPv4-over-IPv6 edge router, IPv4 clouds can connect with the IPv6 clouds. IPv4 protocol is used for communication in IPv4-over_IPv6 intra-domain. Packets will reach the IPv4-over-IPv6 edge router through the IPv4 routing protocol. And the packets will be transformed into pseudo IPv6 packets by the IPv4-over-IPv6 edge router. Based on the IPv6 router protocol, the pseudo IPv6 packets will be routed to the end IPv4-over-IPv6 edge router which then reverted to the IPv4 package and routed to the end node by IPv4 routing protocol.

2.2 The Rule of the Ipv4-Over-Ipv6 Address Mapping

Address mapping is the premise to realize the mutual transformation of the IPv4 and IPv6 packets and routing messages conveniently. The rule of IPv4-over-IPv6 address mapping is as follows: 4over6prefix:IPv4 Address::/v6Len+v4Len, 4over6prefix is the prefix of the IPv4-over-IPv6 mapping address. There are two definitions of IPv4-over-IPv6 mapping prefix nowadays: the first is assigned by IANA, like the 2002::/16 in 6to4; the second is to assign a IPv4-over-IPv6 prefix 2001:250::/32 independently in an autonomous domain shown in the following table.

Table 1. An example of IPv4-over-IPv6 address mapping

IPv4Address	Assigned by IANA 2004::/16	Assigned by AS1 2001:250::/32
202.201.32.0/28	2004:CAC9:20::/44	2001:250:CAC9:20::/60
202.201.32.30	2004:CAC9:201E::	2001:250:CAC9:201E::

2.3 The Process of Packet Transformation

In this section, the transformation of IPv4 and IPv6 packet is analyzed in detail. At present, there are two methods of the packets transformation: packets translation and packets encapsulation. Packets translation[4] [5] is just to translate the IPv4 packet header into IPv6 packet header according to the SIIT [4]principle. Then the IPv4 packet will be translated to IPv6 packet. Packets encapsulation[6][7] is to keep the original packet header and to add a new IPv6 packet header. Then the original IPv4 packet will be transmitted as payload of the new IPv6 packet.

Packets encapsulation can ensure the transparent transition for any operation end to end. But its efficiency is low and the cost of the network is large. Packets translation has less cost and higher efficiency. However it loses information when translating the IPv4 packets header into IPv6 packets header, like IPv4 fragments and IPv4 option information, it may lead to a few special services unavailable.

Both the methods have advantages and the network manager can choose different methods.

2.4 Ipv4-Over-Ipv6 Router Mechanism

The key idea of IPv4-over-IPv6 router mechanism is as follows: Firstly, in the intra-domain of IPv4-over-IPv6, each packet is routed by the standard IPv4 router protocol, like OSPF and RIP. IPv4-over-IPv6 edge router can get the IPv4 routing messages easily through the IPv4 routing protocol. Based on the principle of address mapping in IPv4-over-IPv6, IPv4-over-IPv6 edge router maps the IPv4 routing message into IPv6 and pronounces in the IPv6 network. So the IPv4 routing message infiltrating the IPv6 backbones becomes possible.

Secondly, when an IPv4-over-IPv6 edge router receives a IPv6 router message, revert it into IPv4 router message and inform that to local IPv4 network through the IPv4 routing protocol. Then this process realizes the mutual of IPv4 routing message among IPv4 networks through IPv6 backbones.

3. THE ANALYSIS OF THE ADVANTAGES AND DISADVANTAGES OF IPV4-OVER-IPV6 TRANSFORMATION MECHANISM

3.1 The Advantages of Ipv4-Over-Ipv6 Transformation Mechanism

Related to the transition previous, IPv4-over-IPv6 mechanism is more adapted to the network environment than it was before. It realizes the interconnection of vast IPv4 networks via IPv6 backbone with:

1. High transparency: don't need to do any modification to the IPv4 or IPv6 networks; all works accomplish on the edge router.
2. Excellent adaptability: can complete the selections of adaptability and dramatic router without human interface.
3. Better extensibility

3.2 The Disadvantages of Ipv4-Over-Ipv6 Transformation Mechanism

However, with the development of the network, when the pure IPv6 networks emerge in the IPv6 backbone, some communication problems between pure IPv6 nodes and IPv4 nodes would appear.

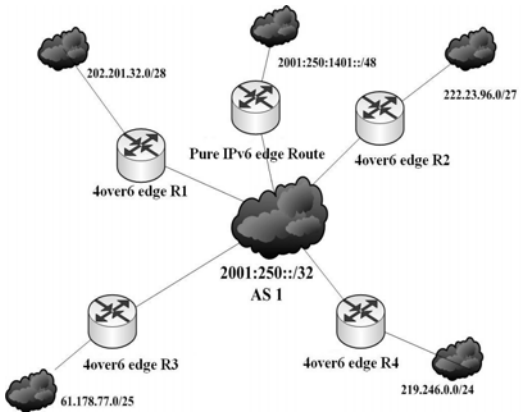


Fig.2. Ipv4 subnets and pure Ipv6 subnets exist together

The details are as follows:

(1) The structure of true IPv6 address and IPv4-over-IPv6 pseudo address is different. The former is composed of IPv6 router prefix and 48 bits MAC address together, but the latter is mapped by IPv4 address. So the true address can not be mapped into IPv4. And the communication can not be established between a pure IPv6 node and a IPv4 node.

(2) In addition, the pure IPv4 applications call IPv4 socksAPI expects to bind an IPv4 address, but there is no valid IPv4 address in the pure IPv6 node. So they can not communicate with IPv4 nodes via pure IPv6 networks.

(3) According to the IPv4-over-IPv6 mechanism, all the works are completed on the IPv4-over-IPv6 edge router. The two possible ways (encapsulation and translation) are unified to set up by administrator according to requirements. However, for IPv6 nodes, there is no unified IPv4-over-IPv6 edge router. The transformation of IPv4-over-IPv6 in pure IPv6 nodes is achieved by themselves and the methods of transformation also need defining by users, but it is so difficult for users also.

4. THE DESIGN OF AN IPV6-OVER-IPV4 EXTENDED MECHANISM

IPv4-over-IPv6 extended mechanism is a good resolution for the limitations of the current IPv4-over-IPv6 mechanism, and it meets the requirements of IPv6 networks' further development.

The design of this mechanism is composed of three parts: the reforming of IPv4-over-IPv6 edge router, the design of IPv4-over-IPv6 negotiation mechanism and the design of IPv4-over-IPv6 intermediate layer driver based on IPv6 node.

The ideas of this design is as follows: after encapsulation of protocol driver, a package will be made and sent to the IPv4-over-IPv6 intermediate layer driver. If the package is IPv6 package, it will be routed to the end via IPv6 networks. If not, a negotiation will be established by negotiation mechanism. When the negotiation completed, the package will be sent to the IPv4-over-IPv6 intermediate layer driver, and transformed into IPv6 package by the driver. Then the package will be routed to

the end IPv4-over-IPv6 edge router by IPv6 routing protocol. When the packet arrives, it will be transformed into IPv4 packet again by the stateful transition mechanism, and routed to the end nodes by the IPv4 routing protocol.

4.1 The Reforming of Ipv4-Over-Ipv6 Edge Router

The reforming of IPv4-over-IPv6 edge router solve the problem of IPv4/IPv6 address mapping which is the basis of interconnection between the IPv4 and IPv6 nodes, describe it in section 3.2(1).

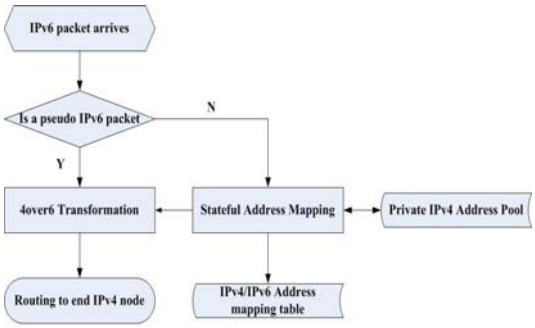


Fig.3. The principle of 4over6 edge router based on 4over6 extended mechanism

The specific method is described in Fig. 3: Establish an IPv4 private address pool which can be routed to IPv4-over-IPv6 edge router, and an IPv4/ IPv6 address mapping table is maintained explicitly. When an IPv6 packet arrives at IPv4-over-IPv6 edge router, the mechanism will judge whether the packet is an IPv4-over-IPv6 pseudo packet or not. If it is, the transformation mechanism will be called directly by the router, if not, a stateful address transformation mechanism router will be called first and then an available address will be taken out from the private address pool, and the address will establish a mapping relation together with IPv6 packet's source address, the mapping relation will be written in mapping table, then the transformation mechanism will be called, and the communications start.

4.2 The Design of Ipv4-Over-Ipv6 Negotiation Mechanism

In the IPv4-over-IPv6 extended mechanism, the design of IPv4-over-IPv6 negotiation mechanism is important for solving the problems of IPv4-over-IPv6 transformation method selecting. An IPv4-over-IPv6 extended header will be designed for the negotiation mechanism, which is shown in Fig 4.

Flag: 00 means requisition; 01 means announcement;
Method: 00 means encapsulation; 01 means translation;
11 means both of them

Fig.4. 4over6 negotiation extended header

When an IPv6 node needs to communicate with an IPv4 node, it will traverse its cache to find a transformation method. If the record is found, the communication would be established. If not, the IPv6 node would send a zero-payload packet including an IPv4-over-IPv6 requisition extended header to end IPv4-over-IPv6 edge router. Then the edge router responds a zero-payload packet including an IPv4-over-IPv6 announcement extended header back. Then the packet will be gotten and the announcement will be written to its cache by the IPv6 node, then the communication will be established by the IPv4-over-IPv6 intermediate layer driver which discussed in section 4.3.

4.3 The Design of Ipv4-Over-Ipv6 Intermediate Layer Driver

In this paper, an IPv4-over-IPv6 intermediate layer driver for IPv6 nodes is designed. The driver is a key component of the communication between IPv6 nodes and IPv4 nodes. The pure IPv4 applications running in the pure IPv6 nodes can be used if the intermediate layer driver is designed. The structure is shown in Fig 5., and the idea as the following: there is an IPv4-over-IPv6 intermediate layer virtual interface to be supported by OS, as the 6to4 and ISATAP does. Because the IPv4-over-IPv6 intermediate layer driver is intervenient between the protocol driver and the NIC driver, echo package have to pass through the driver. If an IPv6 package arrives, the driver does nothing but just send it to the NIC driver directly. If not, the driver transforms the IPv4 package into IPv6 package, and then sends the IPv6 package to the NIC driver.

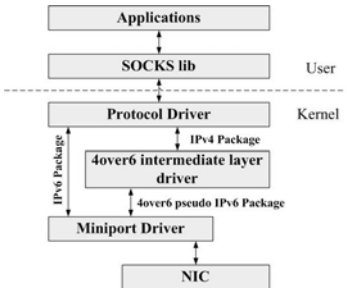


Fig.5. The structure of 4over intermediate layer driver

5. MECHANISM SIMULATION AND RESULT ANALYSIS

5.1 Mechanism Model Building

In order to analyze the feasibility of the idea and test the validity of the mechanism in this paper, a reforming module of IPv4-over-IPv6 based on router and a intermediate layer driver module based on IPv6 nodes are designed in OPNET 10. In addition, an extended mechanism network model of IPv4-over-IPv6 is designed for the simulation; the model is described in Fig. 6.

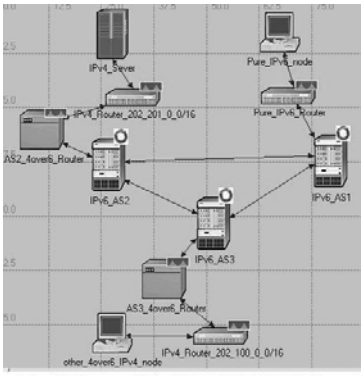


Fig.6. The model of 4over6 extended mechanism simulation

In the case of Fig. 6, three core routers named IPv6_ASx are set as three autonomous domain nucleuses to simulate IPv6 backbone. Pure_IPv6_Router is a pure IPv6 edge router connected with pure IPv6 networks, Pure_IPv6_node is a pure IPv6 node which sets the intermediate layer driver module of IPv4-over-IPv6; and ASx_4over6_Router is the IPv4-over-IPv6 edge router which sets the reforming module of IPv4-over-IPv6; IPv4_Route_xxx_xxx_xxx/x is a pure IPv4 router, and IPv4_Server is a IPv4 FTP server. In the simulation model, it is

interconnected over 1000Mbps among autonomous domains and edge routers. Others are interconnected over 100Mbps.

In this paper, IPv4-over-IPv6 routing mechanism was tested by the routing protocol simulation and the data transmission test was realized by the simulation of File Transport Protocol.

5.2 Simulation and Results Analysis

5.2.1 Simulation of the IPv4-over-IPv6 routing mechanism

IPv4-over-IPv6 routing mechanism will be tested by the methods of routing protocol simulation on Pure_IPv6_Router and IPv4_Route_201_100_0_0/6. Figure 7 summarizes the results.

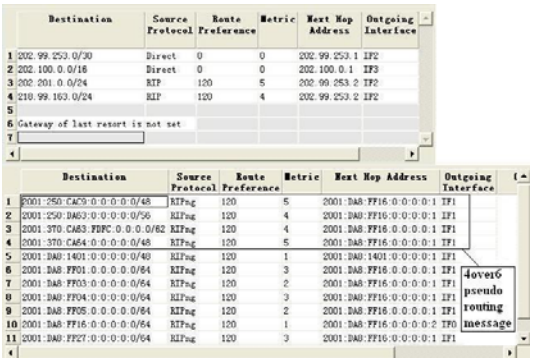


Fig.7. (UP) The result of Ipv4_202_100_0_0/16 routing Protocol simulation
(Down) The result of Pure_Ipv6_Router routing Protocol simulation

From Fig.7, it could be seen that the interconnection addresses 218.99.163.1-2 between the IPv4_Router_202_201_0_0/16, the AS2_4over6_Router have already permeated IPv4-over-IPv6 intra-domain of AS3, and the IPv4 routing message is translated into IPv6 pseudo route message, and received by Pure_IPv6_Router. So the function of routing mechanism is validated under the IPv4-over-IPv6 extended mechanism.

5.2.2 Simulation of File Transmission

In this paper, the communication of application layer protocol is tested by simulation of File Transmission Protocol. Here, a FTP server is set in IPv4-over-IPv6 intra-domain of AS2. The address is 202.201.0.2, and other_4over6_IPv4_node is IPv4-over-IPv6 intra-domain node of AS3, with address 202.100.0.2. The gateway is interface address 202.100.0.1 of IPv4_ 201_100_0_0/6.Pure_IPv6_node is pure IPv6 node. Its address is 2001:da8:1404:30c2:a055:ela4:d5fa and the address of Loopback is a private address 192.168.0.1. The configuration of the Loopback address is not for real communicating, just for encapsulating IPv4 packages. The encapsulated IPv4 packages will be transformed into IPv6 ones by the intermediate layer driver module of IPv4-over-IPv6 based on IPv6 nodes. Simulation result can be seen in Fig. 8.

Fig.8 is a TCP flow picture of Pure_IPv6_node and other_4over6_IPv4_node. From the figure we can draw the conclusion that both IPv4 node and pure IPv6 node can communicate with FTP server of IPv4 normally through the mechanism mentioned in this paper, thus the correctness of this paper's proposals can be validated.

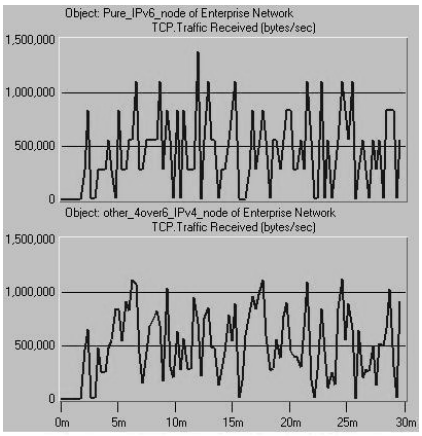


Fig.8. The File transmission simulation of 4over6 extended mechanism

6. CONCLUSIONS

IPv4-over-IPv6 mechanism realizes meets the requirments of vast IPv4 sub network via the IPv6 backbone. However, with the development of the IPv6 network, the pure IPv6 networks should emerg in the IPv6 backbone. In this circumstance, the limitations of IPv4-over-IPv6 mechanism will be exposed.

In this paper, an IPv4-over-IPv6 extended mechanism is designed. It inherits the merit of 4over6 and realizes the transparent communication of nodes in pure IPv6 network and IPv4. Thus, not only IPv4 networks but also networks between IPv6 networks and IPv4 can be interconnected through the IPv6 backbone by the mechanism. Above all, the extended mechanism can be used in the present and coming stages.

REFERENCE

[1] Wu Jianping, Li Xin, Cui Yong，"4over6:IPv4 Network Interconnection over IPv6 Backbone Without Explicit Tunneling." *Chinese Journal of Electronics*, 2006.3, 34(3): 454-458

[2] Huang Dashu, Cui Yong, "Design of 4over6 mechanism based on Solaris 10." *Computer Engineering and Design*, 2007.1,28(1):66-67,117

[3] Wu J, Cui Y, Li X. *4over6 transit using encapsulation and BGP-MP extension*. 2006. draft-wu-softwire-4over6-00.

[4] TSIRTSIS G and SRISURESH P, *Network Address Translation-Protocol Translation* (NAT-PT), RFC 2766,2000.

[5] NORDMARK E, Stateless IP/ICMP Translation Algorithm (SIIT)[S], RFC 2765,2000.

[6] R. Gilligan and E. *Nordmark, Transition Mechanisms for IPv6 Hosts and Routers*, RFC 2893, Aug 2000.

[7] A.. Conta, S. Deering, *Generic Packet Tunneling in IPv6 Specification* , RFC2473, Dec 1998.

[8] Maoke Chen, Xing Li, Ang Li, Yong Cui, "Forwarding IPv4 Traffics in Pure IPv6 Backbone with Stateless Address Mapping",*2006 IEEE/IFIP Network Operations and Management Symposium*,2006:260-270

Jian Song was born in Xu Zhou, Jiang Su province, China, in 1971. He is a associate professor, and dean of the college of Network Education, LanZhou University of technology. His researcher interests are NGN, P2P, and so on.

Mian Huang was born in Jing DeZhen, JiangXi province, China, in 1983. He is a postgraduate of LanZhou University of technology. And his researcher interests are the transition of IPv4/IPv6, MIPv6, and so on

Wei Sun, instructor of LanZhou University of technology, was born in Lan Zhou, Gansu provice,China, in 1973. His researcher interests are IPv6, IPsec, and so on.

Yu Jiao, was born in Luo Yang, He Nan province, China in 1984. Her researcher interests are NGN, Computer Networking, and intelligent Architectural, and so on.

A QoS Routing Protocol Based on Stability and Bandwidth for Mobile Ad Hoc Networks*

Xiangli Wang [1], Layuan Li [1], Bencan Gong [1], and Wenbo Wang [2]
[1]School of Computer Science and Technology, Wuhan University of Technology
Wuhan, Hubei, China
[2]School of Science, Wuhan University of Science and Technology
Wuhan, Hubei, China
Email: wangxiangli@whut.edu.cn

ABSTRACT

The paper proposes a QoS routing protocol based on stability and bandwidth (QRSB) for mobile ad hoc networks. QRSB protocol firstly adopts a bandwidth reservation scheme taking the hidden-terminal and exposed-terminal problems into consideration. Secondly, to select a path with low latency and high stability, QRSB protocol uses a mobile predict method[4]. Thirdly, this protocol adopts two-time reply scheme and reverse optimization of route to improve the routing performance. The location information is provided by global positioning system(GPS). This paper is based on AODV. By QRSB protocol we can get an effective route with a longer life, an enough bandwidth, and a shorter path.

Keywords: MANET, QoS, Routing, Path Stability, AODV

1. INTRODUCTION

A mobile ad hoc network (MANET) is an autonomous system of mobile nodes to establish temporary communication infrastructure for many situations, such as military applications, emergency search, rescue operations and so on. For such networks, topology changes would occur frequently. If this is the case, data must be rerouted quickly, which will introduce more overheads and use more resources. Therefore, to minimize route breaking, we should select stable routes at the beginning that endures a longer time. By taking link stability into consideration in routing protocols[1-4], the routing overheads can be significantly reduced and the QoS performance can be greatly improved.

In addition, the bandwidth is one of the most important requirements in MANETs. The time division multiple access [1](TDMA) scheme is generally used for bandwidth reservation [5-8]. Bandwidth in time-slotted network systems is measured according to the number of free slots. To select feasible paths that satisfy bandwidth requirement, we have to perform a suitable slot assignment strategy.

In this paper, we propose a QoS routing protocol based on stability and bandwidth(QRSB) for MANETs. Firstly, QRSB protocol adopts a bandwidth reservation scheme taking the hidden-terminal and exposed-terminal problems into consideration. This paper is based on AODV. The reason for selecting AODV is that its route discovery mechanism matches the bandwidth calculation scheme very well and is suitable for bandwidth constrained routing. Secondly, to select a path with low latency and high stability, QRSB protocol uses a mobility prediction method[4]. The location information is provided by global positioning system(GPS). Thirdly, QRSB protocol adopts two-time reply scheme of the destination node and reverse optimization of route to further reduce the time of route setup and improve the route stability. By QRSB protocol we can get an effective route with a longer life, an enough bandwidth, and a shorter path.

The remainder of this paper is organized as follows. Section 2 presents the preliminaries. The proposed protocol is proposed in section 3. Experimental results are given in section 4. Finally, conclusions are made in section 5.

2. PRELIMINARIES

2.1 Link Stability Measurement

In this section, we use a mobility prediction method[4] to evaluate link stability. This method uses GPS to get the location information and the mobile speed and direction of a node. Link expiration time(LET) and route expiration time(RET) are two parameters to respectively measure how long a link and a route can keep connected. The final standard of deciding a route is R, which takes both route stability and route length into consideration. The value of R equals to the ratio of RET with hop number. In this paper, we integrate the idea into our protocol.

2.2 Time Slot Information Calculation

The QoS-AODV protocol is on the basis of MAC TDMA protocol[8]. Each MAC TDMA frame consists of two phases, a control phase and a data phase. Each phase is divided into several slots, and several slots form a frame. The control slot is used to transmit control frame. The data slot is used to transmit data frame. To avoid hidden and exposed terminal problem, each node must keep information about itself and its 1-hop and 2-hop neighbors' time slots that are used for sending and receiving. We call a node a neighbor of another node if these nodes are in the transmission range of each other. For a node P, if P wants to send packets, P must calculate the slots that P and P's neighbors don't receive and send packets. The reason of taking P's neighbors into account is to avoid hidden and exposed terminal problems. If P wants to receive packets, it must calculate its free slots that can be used to receive data. These free slots aren't used to receive and send packets from P. The slot scheduling information is exchanged by AODV Hello message.

For a link L, its bandwidth must consider the common free slots of the two neighboring nodes. Two neighboring nodes want to communicate each other. We let one be a sender and let the other be a receiver. The slots that can be used to transmit packets using the link is the intersectant slots that the free slots that can be used to send for sender and the free slots that can be used to receive for receiver.

For a path P, its bandwidth is the minimum link bandwidth of all links along the path P.

3. OUR ROUTING PROTOCOL

Due to the node mobility, the limited bandwidth, and the lack of fixed infrastructure, it is very important to develop an efficient protocol to support QoS requirements in MANETs. In this section, we propose a QoS routing protocol based on stability and bandwidth (QRSB) for MANETs.

3.1 Route Discovery

3.1.1 How Intermediate Nodes Deal With QRREQ Packets

The route discovery process is initiated whenever a source node wants to communicate with another node, and the route table of the source node has no routing information. Our protocol is based on AODV. The source node starts to flood QoS route request (QRREQ) packets with certain bandwidth requirement to its neighboring nodes. When a node has received a QRREQ packet, it performs the following operations:

(1) The node checks whether the value of TTL equals to 0 after the packet arrives at the node and the value of TTL is modified. If yes, the node drops the packet. Otherwise, turn to (2);
(2) The node checks whether itself has been in the node list of QRREQ packet. If yes, the node drops the packet to avoid loop. Otherwise, turn to (3);
(3) The node checks whether the packet is repeated. If it is repeated, the node adopts a reverse optimization of route described later to deal with the repeated QRREQ packet. Otherwise, turn to (4);
(4) The node checks whether link bandwidth satisfies the required bandwidth in QRREQ packet. If not, it drops the QRREQ packet. Otherwise, turn to (5);
(5) The node checks whether the destination node address in the QRREQ packet is its own address. If yes, the node no longer forwards the packet and directly receives it. Otherwise, the mobile node uses the location information in the packet and its own location information to calculate the LET[4]. If we can predict the LET along each link on the route, we will be able to predict the RET, which is the minimum of all LETs along the path.

When the destination node receives a QRREQ packet, it will calculate the value of R for each path. Route selection in the QRSB protocol is based on the value of R. The maximal value of R means a packet is transmitted with a small delay and a high stability.

3.1.2 How Destination Node Twice Replies QRREP Packet

In order to reduce time of routing setup, the destination node will immediately send a QRREP packet to the source node as soon as it receives the first arrived QRREQ packet, because the discovered path in the first arrived QRREQ packet is currently optimized. After a period of time, the destination node maybe receives more other QRREQ packets that come from the same source node. By comparing all discovered routes, the route with the maximal value of R is selected to be the best path. If the best route is not the first replied route, the destination node will reply a QRREP packet again, otherwise it does nothing. The two-time reply strategy[3] can reduce time of route discovery and find a route with a small delay and a high stability.

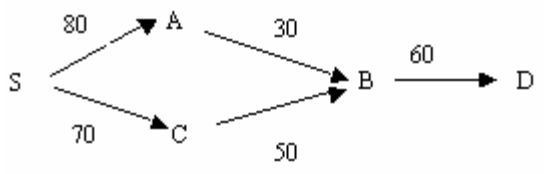


Fig.1. Route discovery process

For example, as shown in Fig.1, the values denoted on each link represent the value of LET. When a source node S wants to transmit data to a destination node D and the routing table of the source node S does not have any information on routing to destination node D, the source node S will broadcast the QRREQ packets to its neighboring nodes A and C. Then the destination node D will receive two feasible paths, which are (S, A, B, D) and (S, C, B D). Among the two paths, we assume path(S, A, B, D) is the first received, whose value of R is min(80,30,60)/3=10. Therefore, the destination node D immediately replies a QRREP packet to the source node in the reverse direction of (S, A, B, D) path, and the source node S starts to send data after it receives the QRREP packet. However, after the destination node receives the other route (S, C, B, D), it also calculates the value of R, which is min(70,50,60)/3=16.7. Having compared the two feasible paths, the destination node decides that path(S, C, B, D) is the most optimized. So the destination node re-sends a QRREP packet to the source node in the reverse of path(S, C, B, D). When the source node receives this QRREP packet, it updates relative route table entry, and sends subsequent data along the best path(S, C, B, D).

3.1.3 Reverse Optimization of Route

In traditional AODV protocol, the intermediate nodes usually drop the repeated QRREQ packets. In our protocol, although the intermediate nodes don't transmit the repeated QRREQ packets, they can make use of local route information of the repeated QRREQ packet to optimize the local route from the source node to the intermediate nodes. When the destination node receives the QRREQ packet and replies a QRREP packet, the QRREP packet maybe is propagated to the source node not along the path that the QRREQ packet comes along.

For example, as is also shown in Fig.1. When the source node S floods QRREQ packets to the destination node D, we assume the QRREQ packet firstly arrives at the intermediate node B along local route (S,A,B). The node B calculates the value of R, which is min(80,30)/2=15, and forwards the packet. After a while, the QRREQ packet with the same sequence number also arrives at node B along local route(S,C,B), and the value R of (S,C,B) equals to min(70,50)/2=25, which is bigger than the value R of (S,A,B). So the intermediate node B modifies its last hop node from A to C, records this change in its route table, and drops the repeated packet. When QRREP packet from the destination node passes by the intermediate node B, the route will be reverse optimized according to the route information of intermediate node. So when QRREP packet reaches the source node, the path is (S,C,B,D) instead of (S,A,B,D). Therefore, data is transmitted along the path(S,C,B,D).

The reverse optimization scheme[3] makes full use of the information of repeated packets to improve route stability. But it also introduces more calculation for each node, and the calculation maybe consumes more power. However, with the development of hardware, the cost of battery is more and more inexpensive. Whereas the communication quality mostly lies on path stability, so more power consumption can be compensated by higher stable path.

3.2 Route Maintenance

Because of high mobility of nodes, links are likely to break, so we must adopt a route reconstruction scheme. Routing reconstruction is usually classified into overall reconstruction and local reconstruction. In this paper, QRSB protocol adopts the local reconstruction[3]. The node, which is on the broken link and is nearer to the source node, initiates a QRREQ packet

to the destination node to reroute, and simultaneously temporarily stores data coming from the source node in the buffer. When the downstream nodes receive the QRREQ packet, they will perform the route reconstruction in the same way as the source node initiates a route discovery process. At the same time, the node, which is on the broken link and is nearer to the destination node, initiates a route-error packet to the destination node to release the reserved slots along the local route the route-error packet has passed by. In this case, QRSB protocol makes full use of existing effective route information, and saves route maintenance overheads.

4. EXPERIMENTAL ANALYSIS

In this section, we use a network simulator to analyze the performance between our QRSB protocol and QoS-AODV[8].

4.1 Simulation Parameters

In our simulation environment, we randomly generated 30 mobile nodes in a 900×900 meters square area. The radio transmission range was set to 250 meters and the data transmission rate was 2Mb/s. We use CBR as data source. The mobile speed was 0~10m/s in random direction. The QoS bandwidth requirement was 2 slots, and each slot was 5 ms. The source node and the destination node were generated randomly. Each simulation time was 800 second. All simulation results are average values of multiple experiments.

4.2 Performance Metrics

The performance metrics mainly include:

(1) Request success rate: The number of successful route requests / the total number of route requests from the source node to the destination node.

(2) Successful transmission rate: The packet number received by receiver / the packet number sent by sender.

(3) Routing overheads: The number of total controlling packets.

4.3 Simulation Results

As is shown in Fig.2 and Fig.3, the request success rate and the successful transmission rate of both protocols fall when the mobile speed of nodes increases. But the performance of QRSB protocol behaves better. The main reason is that QRSB protocol fully takes the path stability into consideration, and selects the route with high stability based on the value of R, so the possibility of link breaking reduces, and request success rate and the successful transmission rate are all improved. On the contrary, QoS-AODV doesn't take path stability into account, so its performance behaves worse. In Fig.4, routing overheads of both protocols increase with the increasing of node mobile speed. However, the routing overheads based on QRSB protocol is lower, because it takes path stability into account, the path is more stable, and the number of routing reconstruction decreases, thus routing overheads correspondingly reduces.

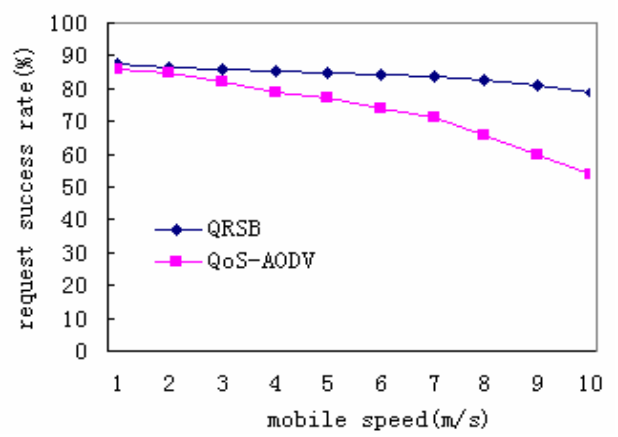


Fig.2. Comparison of request success rate

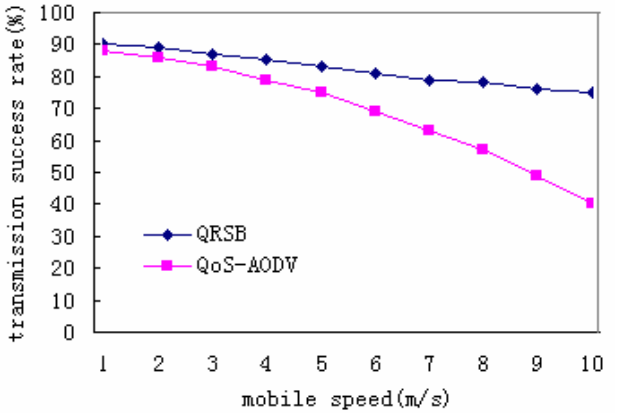


Fig.3. Comparison of transmission success rate

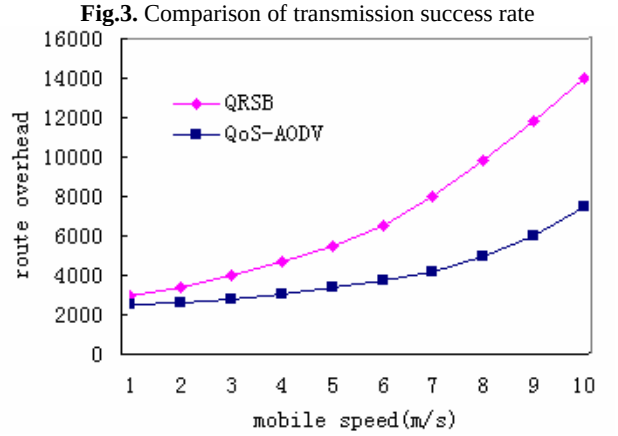


Fig.4. Comparison of routing overheads

5. CONCLUSIONS

The paper proposes a QoS routing protocol based on stability and bandwidth (QRSB) in mobile ad hoc networks. QRSB protocol selects route based on stability parameter R, which greatly improves path stability and reduces the possibility of link breaking. Simultaneously QRSB protocol adopts bandwidth reservation scheme, which further increases the request success rate. Simulation results show that QRSB protocol can provide better performance.

REFERENCES

[1] B.S.Manoj, R.A., C.S.R. Murthy, "Link life based routing protocol for ad hoc wireless networks,"in *proceedings of*

the 10th IEEE International Conference on Computer Communications and Networks,Oct.2001,pp.573-576.

[2] G. Lim, K.Shin, S.Lee, etc,"Link stability and route lifetime in ad-hoc wireless networks," in *proceedings of the IEEE International Conference on Parallel Processing Workshops*,Aug 2002,pp.116-123.

[3] J.Liu,W.Guo,B.L.Xiao and F.Huang,"Path holding probability based ad hoc on-demand routing protocol", *Journal of software (in Chinese)*,vol.18,Mar 2007, pp.693-701.

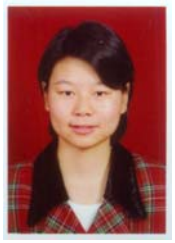
[4] N.C.Wang, and C.Y.Lee, "A reliable qos routing protocol for mobile ad hoc networks with multi-path strategy", in proceedings of *the 14th IEEE International Conference on Networks*,Sept.2006,pp.1-6.

[5] I.J. and J.w., "A race-free bandwidth reservation protocol for qos routing in mobile ad hoc networks", in proceedings of *the 37th IEEE Hawaii International Conference on System Science*,Jan.2004,10pps.

[6] W.H.Liao,Y.C.Tseng and K.P.Shih, "A TDMA-based bandwidth reservation protocol for QoS routing in a wireless mobile ad hoc network", in proceedings of *the IEEE International Conference on Communications(ICC)*, vol.5,2002,pp.3186-3190.

[7] K.P.Shih,C.Y.Chang,Y.D.Chen,and T.H.Chuang, "A distributed slots reservation protocol for QoS routing on TDMA-based mobile ad hoc networks", in proceedings of *the 12th IEEE International Conference on Networks*, vol.2,Nov 2004,pp.660-664.

[8] I.Gerasimov and R.Simon, "A bandwidth-reservation mechanism for on-demand ad hoc path finding", in proceedings of *the 35th Annual Simulation Symposium*, Apr 2002,pp.27-34.



Xiangli Wang, born in 1978, Ph.D. candidate, prelector. Her research interests include high-speed computer networks, QoS routing, and protocol engineering. She has published several technical papers on important journals.

Layuan Li, born in 1946, professor and Ph.D. supervisor. His research interests include high-speed networks, protocol engineering and image processing. Professor Li has published nearly two hundred technical papers and is the author of six books. He was also awarded the National Special Prize by the Chinese Government in 1993.

Accessing Behavior Analysis over IPv4/IPv6 Mixed Networks*

Jinxian Lin [1], Ying He [2]
[1] Network Information Center, [2] College of Mathematics and Computer Science
Fuzhou University, Fuzhou, Fujian 35002, China
Email: [1] jxlin@fzu.edu.cn,[2] hey@fzu.edu.cn

ABSTRACT

The IPv4/IPv6 mixed networks will exist for a long period in the course of the transformation of the currently network into Next Generation Network based on IPv6. In the full study of the feature of the mixed network, an analysis method of users' accessing behaviors is provided over the mixed networks. This method extracts the relevant information from the data stream in the IPv4/IPv6 mixed networks and analyzes the users' behavior eigenvectors by clustering in data mining. Moreover, we design a behavior analyzing model, which provides an effective way for discovering normal behaviors and detecting abnormal behaviors of the network users.

Keywords: IPv4/IPv6 Mixed Networks, Network Behavior Analyzing, Data Streams, Data Clustering, Data Mining

1. INTRODUCTION

With the rapid development of the Internet, the TCP/IP protocol was a huge success. But as the scale of IP network and the number of user continue to growth, the problems caused by IPv4 more and more serious such as address space exhausting and the expansion of routing table, so the Next Generation Network (NGN) based on IPv6 has arisen. Replacing IPv4 by IPv6 couldn't be brought to success in one night and it will exist within a very long time. In order to study the characteristic of traffic or performance and the network behavior model, the research on IPv4/IPv6 mixed network should be put on the agenda. During the transformation of IPv4 into IPv6, the network will be existed in the form of mixed network. IETF IPv6 Transition Working Group (NGtrans) presented some strategies and technology to fulfillment the transition. There are some fairly mature technologies[1,2] such as Dual Stack Technology, Tunnel Technology and Network Address Translation-Protocol Translation. Because of the use of these technologies, the networks contain both IPv4 and IPv6 packets. For the mixed network will exist for a long time, the analysis for the mixed network and its accessing behavior will make the transition gradual and smooth. Further more, this analysis will make great significance in many areas, such as discovering the performance laws of network, forecasting the network behavior, utilizing network resources rationally, keeping away the network attacking and so on.

2. DESCRIPTION OF NETWORK BEHAVIOR

Network behavior is a generalized concept, which indicates the law when the users are using the network resources, it can be described quantitatively and qualitatively by statistic trait or relating relationship of some eigenvector. Analyzing and classifying the user's accessing behavior in real time, we can know the condition of users' operations, the occupying of the network resource and the accessing of data resource in time. All of them can provide feedback information for many tasks, such as the consolidated monitoring of the network resource, the detecting of the system performance and so on.

The key to the network accessing behavior analysis is to establish normal behavior model and to compare the users' current behavior with the model. Then we can judge the degree of the deviation according to the comparison. However, we must describe the behavior efficiently if we want to extract a good model from it. In other words, in order to establish normal behavior model store for the monitored users, we must know the composition of the model store. It means we must choose proper attributes and their relationship to describe the accessing behavior. So we should select some representative attributes from the captured data packets to make them as the descriptive information to be analyzed. In this paper, on the one hand we analyze the frequent degree to obtain the statistic feature of the accessing behavior and on the other hand we analyze some important attributes by the method of data mining.

In general, we use the vector to describe network users' behavior. A user's behavior which contains n attributes can be described as $<attribute_1, attribute_2, attribute_3, \ldots, attribute_n>$, which n attributes are n eigenvalues of the behavior. For example, a browsing behavior can be described as <ID, IP, {URL, Browsing}^{n}> and n>0 is the number of different URL.

In order to describe the formalized network behavior, we use a quadruple[3]: {D, T, *B*, *Q*}. In the quadruple,

- *D* represents the destination address or destination site;
- *T* represents the time when the behavior happened;
- *B* represents the behavior. We use the corresponding ports to describe the different behaviors, such as WWW, FTP, CHAT, TENLET, SMTP, POP3 and so on;
- *Q* represents statistic parameters, such as the size of packet, number of packet and so on.

The quadruple can show the basic feature of network behavior. But for better description, we use discretization to deal with some attributes, by which we will use more abstract data to replace the lower level data. For example, if there is a behavior record like {211.94.144.100, 2007:04:13:09:00, 80, 100}, it is difficult to analysis such a record. So we partition the continuous attributes into several discrete sections and induce the discrete attributes to some different types. For example, the time in a day is divided into some time quantum {MORNING, FORENOON, NOON, AFTERNOON, NIGHT, EVENING}, the sites are generalized according to their topic into some types {DOOR, SEARCH, EDUCATION, FUN, CHAT, SECURITY, OTHER}, and the concrete network behaviors are partitioned based on their destination port into some types {MAIL, FTP, SNMP, WWW, TELNET, POP3, OTHER}. After the above transformation, we can change the foregoing record into {SEARCH, NOON, WWW, 100}. Such transformation is beneficial for us to do the statistic and clustering analysis later.

* The project supported by SSTFFP 2005K007 and MSTSPFP 2005HZ1011.

3. CLUSTING ALGORITHM FOR NETWORK BEHAVIOR ANALYSIS

Clustering algorithm is one of the methods of data mining and it is the computational task to partition a given input into subsets of equal characteristics. These subsets are usually called clusters and ideally consist of similar objects that are dissimilar to objects in other clusters. The input of cluster algorithm is a data set which is composed of one or more data. Each data usually expresses with a vector $(X_1, X_2, \ldots, X_p)$ and X_j represents the value of a continuous or discrete variable. The outputs of cluster algorithm are several clusters, which contains one data at least. A clustering algorithm needs usually to compute the distance or similarity to express the difference between two data.

Definition 3.1 Suppose X_i, X_j were any two data in n dimensional sample space. If function $d(i, j)$ satisfies following condition:

(1) $d(i, j) \geqslant 0$, for all X_i, X_j;
(2) $d(i, j) = 0$, if and only if $X_i = X_j$;
(3) $d(i, j) = d(j, i)$;
(4) Given X_i, X_j, X_k, then $d(i, k) \leqslant d(i, j) + d(j, k)$,

Then we called $d(i, j)$ is the *distance* between X_i and X_j. In this paper, we use Euclidean distance:

$$\sqrt{(x_{i1} - x_{j1})^2 + (x_{i2} - x_{j2})^2 + \cdots + (x_{ip} - x_{jp})^2} \qquad (3\text{-}1)$$

Definition 3.2 The similar degree between two data or samples is called as *similarity* and the similarity can compute through the reciprocal of Euclidean distance[4]:

$$sim(i, j) = \frac{1}{\sqrt{\sum_{k=1}^{p} (x_{ik} - x_{jk})^2}} \qquad (3\text{-}2)$$

For the partitioning method, we use the *k*-means clustering algorithm [6] which adapts to classifying network data streams. The *k*-means requires the input set to be a set of points in the *d*-dimensional Euclidean space. Its goal is to find k cluster centers and a partitioning of the points such that the sum of squared distances to the nearest center is minimized.

The *k*-means algorithm makes the average value of a cluster as the center value of this cluster. The concrete steps of the algorithm can briefly described as follow:

(1) Choosing k data $C_1, C_2, \ldots, C_k$ from the given data set as the initial clustering center of each cluster;
(2) Assigns each data to a set which has the minimum distance to it. Each set is represented by the average value of all the data of it. For each data V_i, find a center C_j to minimize the value of $d(V_i, C_j)$ which represents the distance between them. Then assign V_i to cluster j.
(3) When all the data were distributed in corresponding sets, we need compute the center value (the average value) of each set again;
(4) Repeating execute step 2 and step 3 until the partition of all the data change no longer.

Finally, we will get k sets and each set is a cluster.

This algorithm is a heuristic that converges to a local optimum. The main benefit of *k*-means algorithm is its simplicity and its foundation on analysis of variances. Also, it is relatively efficient. The drawbacks are that the user must specify the number of clusters in advance. The algorithm has difficulties to deal with outliers and clusters that differ significantly in size, density and shape.

4. NETWORK BEHAVIOR ANALYSIS WITH CLUSTING ALGORITHM

4.1 Euclidean *k*-median Method

We use Euclidean *k*-median method[7] to design the clustering algorithm. The general *k*-median problem is described as follow: given a set $\boldsymbol{N}$ of n points, $\boldsymbol{N} = \{x_1, x_2, \ldots, x_n\}$, a distance metric space and an integer k. To use Euclidean distance to compute the distance of two points, we are to choose k members of $\boldsymbol{N}$ as "medians" and assign each member of $\boldsymbol{N}$ to its closest median, which the set of these "medians" is $\boldsymbol{M} = \{m_1, m_2, \ldots, m_k\}$. As before, the assignment distance of a point $x \in \boldsymbol{N}$ is the distance from x to the median to which it is assigned and the *k*-medians objective function, which is to be minimized, is the sum of assignment distances. The formula of the objective function is:

$$\sum_{i=1}^{n} \min_{1 \leq j \leq k} d(x_i, x_j) \qquad (4\text{-}1)$$

Assigning the point and its closest median to a cluster based on these k medians, we can accomplish the task and get k clusters.

4.2 Acquisition of Analytical Data

There are usually two sources of data which we use to analyze the network accessing behavior. The one is based on host, the other one is based on network. The former is come from the audit records of operation-system or the server log. In this paper, we use the later, which is come from the network data stream. The objects of analysis are network packets which were captured from real data stream by the technology of network monitoring.

The primitive captured packets are not suitable for doing clustering analysis, so we need describe the network accessing behavior by vector. We can extract useful information from the primitive network packets to compose the accessing records. Each record represents a TCP/IP connection record, which contains several attributes, such as network protocol, connection time, destination/source IP address, port number and so on. So we can use such record which contains several attributes to make up of the vectors for clustering analysis.

There are many types of attribute data in the network accessing record, such as numeric data, boolean data, enumerate data and so on. In this paper we will compute the distance according formula (3-1) for which only the numeric data is suitable. So we will do some special changes with such data: when a attribute k in data x_i and x_j is not a numeric data, if $x_{ik} \neq x_{jk}$, we use a constant to replace the value of $(x_{ik} - x_{jk})^2$, otherwise set the value of $(x_{ik} - x_{jk})^2$ as zero.

4.3 Analysis of Accessing Behavior

The user' single behavior often is accidental. In order to get the feature of users' behavior we should analyze a mass of behavior. In this paper we extract the basic feature of users' behavior by statistic method, which include the traffic statistic of concrete accessing behavior and concrete visiting sites in a period of time.

In section 2 we narrated a quadruple method to describe users' accessing behavior. A record represents a visit behavior. If we do statistic analysis for several behavior in a period of time, we can get the user' traffic feature in this period of time. The concrete contents are as follow:

(1) The total packets length and number of which the monitored IP had sent out;

(2) The total packets length and number of which the monitored IP had sent out to each destination site. Then calculates respective percentage according the value of step one;
(3) The total packets length and number of which the monitored IP had sent out to each destination port. Then calculates respective percentage according the value of step one.

For example, Tab.1 is the statistic result of a user's behavior in thirty minutes.

Table 1. The statistic result of a user's behavior

R	*T*	*Door*	*Search*	*Edu*	*Fun*	*Other*	*N*
1	30*m*	30%	30%	10%	10%	10%	1200

In Tab.1, *R* is the number of record; *T* is time and the unit is minute; *Door* is the accessing percentage of the site belongs to door site; *Search* is the accessing percentage of the site belongs to search site; *Edu* is the accessing percentage of the site belongs to education site; *Fun* is the accessing percentage of the site belongs to fun site; *Other* is the accessing percentage of the site belongs to other types of site; *N* is the number of packets.

Tab.1 tells us the traffic percentage of each type site has occupied in the total 1200 packets in thirty minutes. We partition all the sits to these types: Door, Search, Education, Fun and Other.

It is very convenient for us to do the clustering analysis after the above traffic statistic analysis.

4.4 Data Standardization

To adopt cluster algorithm, we need to carry on the standardization to the attribute value, for there may are many differences between the attributes values and moreover they use the different unit to measure. For example, the unit of time may be second or minute. With the different measure method, the influence on the distance between data is also different. In order to eliminate the influence on distance caused by the different measure method, we needs do the standardization. The concrete method is as follow.

At first, compute the value of *m* and *s*, which *s* stands for the average value of each attribute and *m* stands for the average absolutely offset of each attribute.

$$m_i = (x_{1i} + x_{2i} + \ldots + x_{mi}) / n \quad (4\text{-}2)$$

$$s_i = (| x_{1i} - m_i | + | x_{2i} - m_i | + \ldots + | x_{mi} - m_i |) / n \quad (4\text{-}3)$$

m_i stands for the average value of attribute i and s_i stands for the average absolutely offset of attribute i. $x_{1i}, x_{2i}, \ldots, x_{mi}$ are the values of attribute i in each data. Then do the standardization to every data:

$$Z_{ji} = (x_{ji} - m_i) / s_i \quad (4\text{-}4)$$

Z_{ji} is the value of attribute i of data j.

In fact, this kind of transformation change the data from its originally space to a standard space.

4.5 Improvement to *k*-median Method

In this paper, we use Euclidean distance as formula (3-1). After computing experiment data, we founded a problem that some small value but important data were covered by the data which have big value in the vectors. For example, there are three records which were obtained by using the method described in section 4.3, as showed Tab.2.

Suppose record 1 in Tab.1 is a cluster median, now we want to compute the distance between 2, 3 and 1 respectively according formula (3-1).

Note: in order to compute conveniently, we multiplied the percentage data by 100.

Table 2. The example of users' behavior

R	*T*	*Door*	*Search*	*Edu*	*Fun*	*Other*	*N*
1	30*m*	10%	40%	40%	5%	5%	1200
2	40*m*	10%	5%	0	80%	5%	1500
3	40*m*	5%	40%	45%	0%	10%	4200

$$d(1, 2) = \sqrt{10^2 + 0 + 35^2 + 40^2 + 75^2 + 0 + 300^2}$$

$$= \sqrt{98550} \quad (4\text{-}5)$$

$$d(1, 3) = \sqrt{10^2 + 5^2 + 0 + 5^2 + 5^2 + 5^2 + 3000^2}$$

$$= \sqrt{9000200} \quad (4\text{-}6)$$

We can see that $d(1, 3) > d(1, 2)$, which explain that the behavior described by record 2 is more similar to the median (record 1) than record 2. But after anatomize the three records, we can see directly that record 3 is more similar to record 1 than record 2. Because their accessing sites mainly concentrates in education and search sites and the record 2 mainly concentrates in fun sites, $d(1, 3) > d(1, 2)$. It is because the value of the last attribute is very big and its magnitude is far bigger than other attributes, which reduced the weight of other attributes in the distance.

In this paper we use weighted distance to improve the Euclidean distance. The weighted Euclidean distance can reduce the influence on distance caused by the different magnitude of the attribute.

$$d(i, j) = \sqrt{w_1(x_{i1} - x_{j1})^2 + w_2(x_{i2} - x_{j2})^2 + \cdots + w_p(x_{ip} - x_{jp})^2} \quad (4\text{-}7)$$

$(w_1, w_2, \ldots, w_p)$ is the weight vector. In this example, we want to reduce the magnitude of the last attribute, so we set the weight of the last attribute $w_7 = 1/100$ and set the weight of other attribute $w_i = 1$. After the introduction of weight, we will get a new table Tab.3 from Tab.2.

Table 3. The example of users' behavior with weight

R	*T*	*Door*	*Search*	*Edu*	*Fun*	*Other*	*N*
1	30*m*	10%	40%	40%	5%	5%	12
2	40*m*	10%	5%	0	80%	5%	15
3	40*m*	5%	40%	45%	0%	10%	42

Then we can get the new distance between these records:

$$d(1,2) = \sqrt{10^2 + 0 + 35^2 + 40^2 + 75^2 + 0 + 3^2}$$

$$= \sqrt{8559} \quad (4\text{-}8)$$

$$d(1,3) = \sqrt{10^2 + 5^2 + 0 + 5^2 + 5^2 + 5^2 + 30^2}$$

$$= \sqrt{1100} \quad (4\text{-}9)$$

We can see that the $d(1, 3) > d(1, 2)$ after using the weighted Euclidean distance, so we can conclude that the improvement is effective.

5. BEHAVIOR ANALYSIS MODEL OF MIXED NETWORK

According to the characteristic of IPv4/IPv6 mixed network and together with the analysis method narrated above, we

proposed a behavior analysis model of mixed network. The Fig.1 is the model.

The Data Acquisition module is primary for gathering the analysis data. We use the network monitor technology to capture the network packets from network data stream.

The Packets Pretreatment module is used for doing the standardized processing to the captured data, which will discard some data that the users are not interested in. For the characteristic of IPv4/IPv6 mixed network, the format of packets in data stream are different, so we need do this processing to let the packet accord to only one format, which will be IPv4 or IPv6.

In order to get the analysis eigenvector, we need to fetch information from some fields in the captured packets. According to the feature of mixed network, we should treat the packets of IPv4 or IPv6 respectively. We may fetch such fields as destination IP address, source port number, protocol information and so on. Meanwhile we can do the statistic analysis. All the above works will be done in these two modules: IPv4 Protocol Analysis and IPv6 Protocol Analysis.

The Behavior Analyzer is used for accomplishing the clustering analysis. We will use clustering algorithm to analysis the information which were obtained by the forenamed modules. After analyzing a mass of users' behavior, we can construct the user behavior outline.

The Behavior Outline is constructed by analyzing the commonness of a mass of users' accessing behavior. We can accomplish the discovering of normal behavior and the detecting of abnormal behavior by comparing the current behavior to the outline.

The Result Treatment module mainly is used for providing feedback information for the network monitoring and offering reasons for active management for the network.

6. CONCLUSIONS

In this paper, we discussed the describing and analyzing method of users' behavior based on our research on network accessing behavior according to the characteristic of the IPv4/IPv6 mixed network. We used Euclidean *k*-median method to do the clustering analysis on users' accessing behavior and do some improvement on this method. Moreover, we proposed an analysis model of user' behavior, which will provide reasons for controlling and active managing the mixed network.

REFERENCES

[1] *Transition Mechanisms for IPv6 Hosts and Routers,* RFC 2893.
[2] *Network Address Translation-Protocol Translation,* RFC 2876.
[3] Li W., "Network Security Framework Based on User Behavior Analysis", *Computer Engineering and Applications*, 2002 (12): 163-164.
[4] J. R. Jang, C. T. Sun and E. Mizutani, *Neuro-Fuzzy and Soft Computing*. New York: Prentice-Hall, 1997. 423-433.
[5] Zhu M., *Data Mining*, He Fei, University of Science and Technology of China Press, 2001.
[6] K. Alsabti, S. Ranka and V. Singh. "An efficient *k*-means clustering algorithm". *In Proc. of the First Workshop on High Performance Data Mining, Orlando,* FL, March 1998.

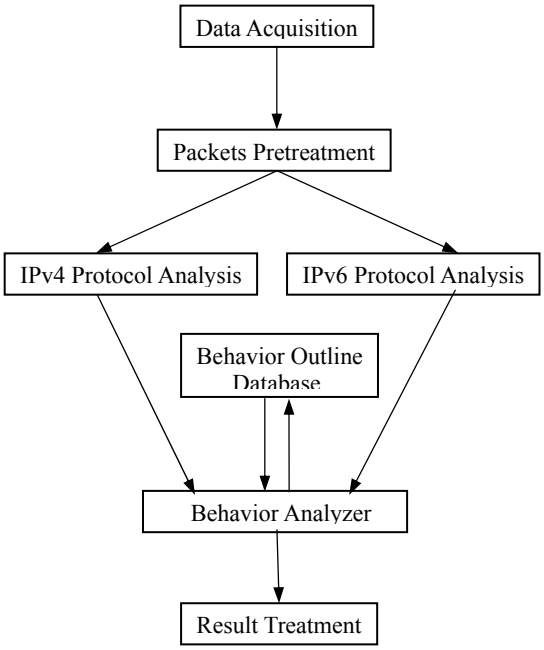


Fig.1. Behavior analysis model of mixed network

Jinxian Lin is a Associate Professor and a head of Network Information Center, Fuzhou University. He was graduated from Fuzhou University as a bachelor in 1982 and from Xi'an Jiaotong University as a doctor in 2004. He has published over 50 Journal papers. His research interests are in network information system and database system.

Ying He is master candidate in Fuzhou University. His current interest includes in network information system.

A Prediction-based QoS Routing Protocol in Mobile Ad Hoc Network with Unidirectional Links *

Jin Lian[1,2], Layuan Li[1] ， Xiaoyan Zhu[2]
[1]School of Computer Science and Technology, Wuhan University of Technology
Wuhan, 430063, P.R.China
[2]School of Mathematics & Computer Science, JiangHan University
Wuhan, 430056, P.R.China
Email: lj_jhun@163.com

ABSTRACT

Due to the hidden terminal, the bidirectional links sometimes become the unidirectional links in mobile ad hoc network (MANET). The QoS (Quality of Service) routing is the process for establishing the path which is from the source to the destination with multiple QoS constraints. The paper presents a prediction-based QoS routing protocol in mobile ad hoc network with unidirectional links (PQRPU).The PQRPU attempts to reduce the overhead for reconstructing a routing path with multiple QoS constraints by mobile predicting. In this paper, the proof of correctness of the PQRPU is also given. The simulation results shows that the PQRPU approach provide an accurate and efficient method of estimating and evaluating the QoS routing stability in dynamic mobile networks.

Keywords: Qos, Motion Predicting, Unidirectional Link.

1. INTRODUCTION

The mobile ad hoc network (MANET) is communication network formed by mobile radio-equipped terminals without a fixed infrastructure in such way, that each communicating device can serve as a router for the others [1- 4]. All the nodes are free to move around randomly, thus changing the network topology dynamically [6]. The traditional routing protocol used wired networks are not suited for MANET. At present, many applications need to provide quality of services (QoS). In MANET, QoS routing protocol has been a research hotspot and presented by many scholars. These protocols can be broadly classified into table-driven and on-demand QoS routing protocols [5,8]. The typical QoS routing protocols is TBP (Ticket-Based Probing) [5] and CEDAR (Core-Extraction Distributed Ad Hoc routing) [7].But these QoS routing protocols are used in MANET with full-duplex directed wireless communication links. Due to the characteristic of MANET (such as hidden station problem, environment disturb etc), the bidirectional link sometimes becomes the Unidirectional link. In order to solve the problem, some scholars have presented the schemes. For example, Prakash R and Singhal M present the ARUL [2] scheme. Zang w.y. also presents the UAOR [4] method. In these routing protocols, the QoS is not taken into account.

Link Status Predicting can discover a Stability routing and avoid low quality paths. The basic idea is firstly to find some Stability routing paths, and then according to the realistic traffic of node maintain routing paths. Therefore, we can guarantee performance with realistic accuracy.In this paper, we present a Stability Routing with Link Status Predicting in Mobile Ad hoc Network (LSPRP).

This study presents a prediction-based QoS routing protocol in mobile ad hoc network with unidirectional links (PQRPU).Adopting motion predicting mechanism, the PQRPU chooses the most stable routing path which satisfies the QoS constraints in mobile ad hoc network with unidirectional links. It adopts the on-demand strategy to establish and maintain route. The PQRPU reduces the overhead for reconstructing a routing path, increases the success rate of packet transmission.

The rest of the paper is organized as follows. Section II describes the network model and motion predicting mechanism. Section III presents a prediction-based QoS routing protocol with unidirectional links (PQRPU), Simulation results is in section IV. Section Ⅴ describes the conclusion.

2. NETWORK MODEL WITH QoS DEFINITION

When the routing problem is researched, the network can be denoted by the graph with weight—G (N, E), where N is the collection of the nodes and E denotes the collection of the communicating links. |N| and |E| denote the number of the nodes and links, respectively [9]. The network model only considers universality, namely there is not more than one link between the two nodes.

Definition1. For $\forall n_i \in N, \forall n_j \in N$ and $n_i \neq n_j$ in G(N,E), (i , j) denotes the link between n_i and n_j .In MANET with unidirectional links, for $\forall(i,j) \in E$,there exists $(j,i) \notin E$ or $\exists(i,j) \in E \wedge (j,i) \notin E$.

Definition2. The model only takes into account the QoS constraints of the links, since the node and the link is equivalence. Assume $p(s,d)$ denotes a path form the source to the destination, where $s \in N$ and $d \in (N - \{s\})$. Assume R is the collection of positive real number and R^+ is the collection of non- negative real number. For $e \in E$, the metrics of QoS is defined by functions as followed:

$delay(e): E \to R$

$\cos t(e): E \to R$

$bandwidth(e): E \to R$

$delay - jitter(e): E \to R^+$

Then the QoS of the whole path is defined:

* This work is supported by a grant from National Natural Science Foundation of China (No.60672137), the Ph.D. Programs Foundation of Ministry of Education of China (No.20060497015), NSF of Hubei Province of China (No.2006ABA301).

$$delay(p(s,d)) = \sum_{e \in p(s,d)} delay(e) \quad (1)$$

$$bandwidth(p(s,d)) = \min\{bandwidth(e), e \in p(s,d)\} \quad (2)$$

$$delay - jitter(p(s,d)) = \sum_{e \in p(s,d)} delay - jitter(e) \quad (3)$$

Definition3. The QoS that has selected the routing path must satisfy promissory QoS constraints, namely:

$$\begin{aligned} &delay(p(s,d)) \le D \\ &bandwidth(p(s,d)) \ge B \\ &delay - jitter(p(s,d)) \le DJ \end{aligned} \quad (4)$$

where D, B and DJ denote the delay constraint, bandwidth constraint and delay jitter constraint, respectively.

3. PQRPU

Due to the mobile ad hoc network with unidirectional links, the design of PQRPU is considered especially. In PQRPU, the neighboring nodes use GPS to communicate each other in order to obtain a stable routing path by motion predicting mechanism. Simultaneity, the routing discovery of PQRPU searches a path form the source to the destination with multi-constraint QoS. The routing maintenance is to renew the path as soon as possible. The correctness proof of PQRPU is given in the end.

3.1 Motion Predicting Mechanism

In mobile ad hoc network, the reliability of a path depends on the stability or availability of each link of this path because of the dynamic topology changes frequently. It assumes a free space propagation model [10], where the received signal strength solely depends on its distance to the transmitter. Therefore, using the motion parameters of two neighbours (speed, direction, and the communication distance), the duration of time can be determined in order to estimate that two nodes remain connected or not. Assume two nodes i and j are within the transmission distance r_a of each other. Let (x_i, y_i) and (x_j, y_j) be the coordinate of mobile host i and mobile host j. Also let (v_i, θ_i) be the speed and the moving direction of node i, let (v_j, θ_j) be the speed and the moving direction of node j. The LET (Link Expiration Time) is predicted by [10]:

$$LET = \frac{-(ab+cd) + \sqrt{(a^2+c^2)r_a{}^2 - (ad-bc)^2}}{a^2+c^2} \quad (5)$$

where

$$\begin{aligned} a &= v_i \cos\theta_i - v_j \cos\theta_j \\ b &= x_i - x_j \\ c &= v_i \sin\theta_i - vj \sin\theta_j \\ d &= y_i - y_j \end{aligned}$$

Note that when $v_i = v_j$ and $\theta_i = \theta_j$, LET becomes ∞. In other words, if LET is ∞,the link will remain connected at all times. On the other hand, if LET is negative, the link is disconnection.

3.2 Process of PQRPU

In MANET with unidirectional links, PQRPU includes two phases—routing discovery and routing maintenance. The routing discovery searches a path form the source to the destination with multi- constraint QoS. When the path is disconnection, the routing maintenance is to renew the path as soon as possible. The routing request packet includes the following options as follows: S-address, D- address, sequence, position, speed, moving direction of the mobile host, D, DJ, B.

The process of routing discovery is following:

Step1: if the routing table of source node exists the route to the destination, the message is directly sent to the destination. Otherwise, the source broadcasts for the destination by routing request packet.

Step2: if the received routing request packet is a duplicate, the midst-node discards the routing request packet. Otherwise, go to step3.

Step3: if $bandwidth(e) \ge B$ and the midst-node is not the destination, the midst-node forwards the routing request packet. Otherwise, the midst-node discards the packet.

Step4: according to step1—step3, the destination can obtain the collection of the route from the source to the destination.

Step5: delete some route from the collection which is not satisfied $delay(p(s,d)) \le D$ and $delay - jitter \le DJ$.

Step6: if the collection is not empty, the destination selects the routing path that has the biggish LET and sends the routing replay to the source. (When sending the routing replay to the source, if the link is unidirectional, the node can broadcast.) Otherwise, the destination sends routing- reconstruct information to the source.

Due to the dynamic nature of the network topology and restricted resources, the established route often becomes invalid. When the link is disconnection, the upriver-node sends routing- reconstruct packet to the source. The source starts to discovery the route over again. If the source receives routing- reconstruct packet and routing reply packet at the same time, the source discards the routing reply packet and deals with routing- reconstruct packet.

3.3 Correctness Proof of PQRPU

Theorem 1. In *PQRPU*, some links of the network model are the unidirectional links, denoted by G = (V, E).For $\forall n_i \in V, \forall n_j \in V$ and $n_i \ne n_j$, if n_i wants to send message to n_j , n_i can obtain the routing path form n_i to n_j by sending routing request.

Proof: If $(i,j) \in E \wedge (j,i) \in E$, n_j can apparently receive the routing request form n_i .If $(i,j) \in E \wedge (j,i) \notin E$ or $(i,j) \notin E \wedge (j,i) \notin E$, n_j can receive the routing request form n_i and n_i can also receive the routing reply form n_j because the network graph is a strong connected graph. Although the QoS and the link stable predicting are involved in routing establish, the correctness of PQRPU is not influenced because some information (QoS metrics, parameters on motion predicting) are added in the routing request packet

Theorem 2. If a certain routing path is invalid in unidirectional mobile ad hoc network, the source can receive the routing disconnection information in the process of routing maintenance.

Proof: If the source is still in the network, the routing disconnection information can be always sent to the source because the network graph is a strong connected graph. When the source is moving in the direction of being close to the

disconnection link, the source can receive the routing disconnection information. But if the source is moving in the direction of being away form the disconnection link and is not in the communication range, the source can know the routing invalidation although it can not receive the routing disconnection information.

4. SIMULATION

4.1 Simulation Environments

The simulation model a network by randomly placing mobile nodes within $1000m \times 1000m$ area. The radio propagation range for each node is 250 meters. Each simulation is executed for 500 seconds of simulation time. A free space propagation model is used in the experiments. A traffic generator is developed to simulate CBR sources. The size of data packet is 512 bytes. Data sessions with randomly selected sources and destination are simulated. Each source transmits data packets at a minimum rate of 5 packets/sec and maximum rate of 10 packets/sec. In simulation, assume $D \le 0.5$, $DJ \le 1.0$ and $B \ge 2000Hz$.

4.2 Simulation Result

In order to evaluate the performances of the PQRPU, The proposed scheme is simulated in ns-2[11].During the experiment, the research PQRPU mainly from the cost of control packet, the success rate of data transmission.

Fig.1 depicts a comparison of data transmission success rate for UAOR and PQRPU when the nodes very its movement speed. The success rate of data transmission in PQRPU is higher than in UAOR, which means it is more suitable for the routing choosing under timely data transmission application nd dynamic network structure. When the speed of nodes increases, the network topology changes faster. In other words, owing to the increase of the node's speed, some route paths may become invalid. So it reduces the success rate of data transmission. But PQRPU adopts the mobile predicting mechanism in order to establish the stable links, provides a quick response to changes in the network. The cost of control packet is shown in the Fig.2. It proves that the cost of control packet reduces because the number of routing request and routing replay reduces.

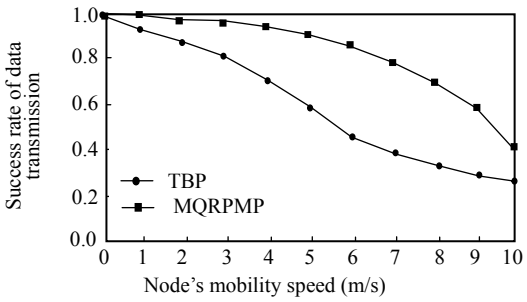


Fig.1. Success rate of data transmission vs. Node's mobility speed

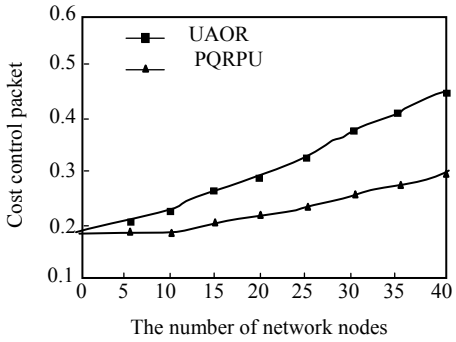


Fig.2. Cost control packet vs. Number of network nodes

5. CONCLUSIONS

This paper discuss the problem of QoS constraint route, deals with the delay, delay jitter and bandwidth metrics. It describes the networks model with unidirectional links, presents a prediction-based QoS routing protocol in mobile ad hoc network with unidirectional links (PQRPU).The PQRPU can select the stable route form source node to the destination by mobile predicting, and this routing path satisfies multiple QoS constraints according to the QoS demand. The PQRPU provides a quick response to changes in the network, minimizes the waste of network resources, produces significant improvements in data transmission rate, and reduces the overhead for reconstructing a routing path. In the paper, the correctness proof of PQRPU is given. The simulation results demonstrate the proposed approach.

REFERENCES

[1] Jüttner, A. and Magi, Á. "Tree Based Broadcast in Ad Hoc Networks." *Mobile Networks and Applications*, Vol10, No.5,2005, pp.753-762.

[2] Prakash R, Singhal M. "Impact of unidirectional links in wireless ad-hoc networks" [A]. In *Proc DIMACS Workshop on Mobile Networks and Computing* [C]. Rutgers University, NJ. 1999, pp.272-281.

[3] Sun, B.L.: "long-life multicast routing protocol in MAODV based on entropy." *Journal of Computational Information System*,Vol1, No 2,2005, pp.263-268.

[4] Zang W Y, Yu M and Xie L. "A routing protocol for ad-hoc mobile network with unidirectional link"[J].*Chinese Journal of compute*, 2001, 24(10), pp.1018-1025

[5] S. Chen, K. Nahrstedt: "Distributed Quality-of-Service Routing in Ad Hoc Networks." *IEEE Journal on Selected Areas in Communications* 17(8),1999, pp. 1488-1505

[6] Sun B. L., and Li L. Y., "A QoS Based Multicast Routing Protocol in Ad Hoc Networks," *Chinese Journal of Computers*, vol. 27, No.10, pp.1402-1407, 2004(in Chinese).

[7] J. Broch, D. B. Johnson, D. A. Maltz: *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks* (Internet draft), 1998.

[8] S.K.Shah, K. Nahrstedt: "Predictive Location-based QoS routing in Mobile Ad Hoc Network." *Proceedings of IEEE International Conference on Communications* (ICC 2002).New York., Vol.2,Aug 2002, pp. 1022-1027.

[9] Li L. Y., Li C. L. *A Dynamic QoS Multicast Routing*

Protocol. ACTA ELECTRONICA SINICA, 2003, 31(9), pp.1345-1350(in Chinese).

[10] William Su,Sung-Ju Lee, and Mario Gerla: "Mobility Prediction in Wireless Networks." *21st Century Military Communications Conference Proceedings*. (MILCOM 2000). Los Angeles, CA, USA, Vol1, Oct 2000, pp.491-495.

[11] *The NS Manual*, A Collaboration between researchers at UC Berkeley,LBL,USC/ISI and Xerox PARC. Available at http://www.isi.edu/nsnam/ns.

A Study and Design of Call Model in Mobile Softswitch *

Zhuping Hua [1,2] , Qiuyu Zhang [2]
[1.]Wuxi Professional College of Science and Technology Wuxi, 214028
[2.]School of Computer and Communication Lanzhou University of Technology,Lanzhou, 730050
Email: Hzpalqy@163.com

ABSTRACT

Call model is the core in mobile softswitch design. On the basis of analyzing existing mobile softswitch call model, a distributed MSC-Server call model. is put forwrad. This model realized mobile station initiate the forward direction bearer establishment call control flow and route selection, This call-controlling model realizes the separation of call control and medium bearer, and the separation of service logic and call control, and itt allows the accessing of multi-protocols, making call control indepent of of underlying bearer potocols, and thus meeting the needs of the call control in mobile softswitch.

Keywords: Call Model, MSC-Server, Route Selection, Mobile Softswitch

1. INTRODUCTION

The softswitch is the control function entity of the NGN[6][7], which is the core device of evolution of network be exchanged from the circuit network to the distributed network of beared with IP. Satisfied the function of NGN' real-time request of business provide, call control and link control, which is a technical core of the NGN. The softswitch is independent on the main function of beared protocol in the ground floor, completedthe call control, the accessed control of media gateway, resources distribution, protocol processing, routering, authentication, accounting etc, and could provide all business that existed in electric circuit and the diversify third business, which has already become the development direction of the next generation fixed network, also become the an important technique for adopted of the next generation mobile Network. Softswitch technique combine with mobile core network have numerous superiority technically. But in mobile network, for sustaining ambulation under various environment, need exploitation the network function in control layer. Especially Identify and confirm mechanism、connection control and authorization、 position management, terminal and the distribution and management of contaction address、 sustain the management of customer environment、the management of the customer capability and access to the management of the customer data[5].Increased the difficulty to execute mobile softswitch system.This paper put forward a mobile softswitch call model based on the distribution MSC electric circuit structure.

2. THE REQUEST OF CALL MODEL

This model based on the design of softswitch technical, made the valid separation of call control and business bear. Realizd the connection of all IP inner, Satisfied with the NGN system structure and communication network of all IP turn the direction development.Aim at its characteristics, build up a fit ambulation softswitch call model to need according to the following what is requested:

(1) Interinfiltrate and intercommunication request of network: Softswitch need to realize admission of the multi-isomerism network and back up many different network protocol.So do the mobile softswitch network.If every protocol needs to build up independent calling control about itself，it will be more complex and discommodious to interinfiltrate. This will be opposite to what we want. So we need to abstract the feature of the network protocol, build up universal call control model on network source layer and realize the network co-communication on concentrated controlling layer by dealing with the different protocols universally. Realizing softswitch needs to back up manyprotocols'jointless co-communication such as H.248/Megaco、MGCP[4]、H.323、SIP、ISUP、PRI、SIP-T/SIP-I[1]-[3].

(2) Bearer connection control: The main idea of the mobile softswitch is realizing the separation of the call controll and the bearer. The management of the Connection Bearer is more complex than the way of the single switched circuit. There are two basic bearer medium in mobile softswitch: TDM-based circuit channel with 64 kbit/s and IP-based RTP real time media flow. The mobile softswitch must support the transition and co-communication of both TDM-based and IP-based media flow, it also must support the selection of the load supporting media and the selection of the loading ways to the calling. So the design of the call model must include the independent media load supporting management module, complete the management of the media source and media circuit, and insure the needs of some affairs about the service quality.

(3)Supporting of the server ability: The design of the mobile softswitch must embody the mentality of the server driving. Upper layer server has no relation with the isomerous network of the bottom layer must be embodied. Provide exoteric and mobile server providing system. Realize the co-communication relating with present server network such as intelligent network. Inherit the present mature communication server. Realize all the server of the traditional exchanger into the softswitch. At the same time provide supporting to data server, multipartite, multimedia server ability and the detecting of the server conflict. The exoteric server system uses the way of next network server providing which is based on API. We have the present mature API, such as Parlay [8], JAIN. The design of the call model must be convenient to map the API like Parlay and supports the intelligence network INAP protocol API.

3. CALL SYSTEM MODEL

The call system model is based on distribution system structure as Figure1. We produce a kind of mobile softswitch model which the sever and controlling are separated. In this model, traditional MSC is composed of MSC Server, GMSC Server and MGW. MSC Server and GMSC Server provide function of call controll and mobile management. MGW provides function of media controll and source transaction. MSC Server is

* Gansu Province Programs for Science and Technology Development, (2GS047-A52-002-03)

composed of CDC(circuit distribution controller) and CS(call server). GMSC Server is composed of CMG,, CSG and IP network equipments.

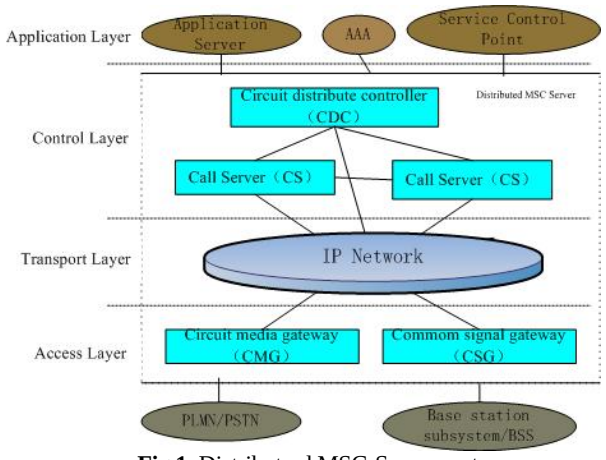


Fig.1. Distributerd MSC-Server system

Every part communicates with each other by IP network. In the mobile softswitch model system, MSC Server is connected to the gateway with MGW and AG and completes the traditional MSC function of PLMN. Softswitch supports BSSAP by SIGTRAN and by connecting AG and BSC. The function of CDC is to statistic routing and calling information, to deal with the using of circuit source, and to assistant CS to complete the connecting control of every server. CS completes the controll and management of the circuit, and provides SIG controll function and manages other sources. CMG is mainly responsible for bearer and the management function relating with relay circuit physical state. The system disposes many CS and CMG, makes a distributivity system structure. Thinking about the load and the management direction, every CS is responsible for management of circuit sources in one or more CMG.. As SG equipment, CSG is SG proxy equipment which is used to send and receive messages in the edge of NO.7singal network and IP network. Its function is relay translating and completing messages in the gateway of the SG and IP network.

In function, NGN entity is composed of four layers: sever layer, control layer, transaction layer, access layer. In this model, function entity like application sever and AAA sever SCP all belong to the server function entity in the mobile network system. And provide increment server, server exploring plan and the third part programmed API function. CS and CDC are located in control layer providing functions of call controll and connection controll. IP network belongs to transaction layer, it is used for load supporting media stream and high bid-width grouped network. Both MG and SG belong to media access layer, they can realize the connection of access and SG between different severs by using different cutover equipments. Thy also can realize the transaction of message format. In this system, CS and MG can communicate with each other by using the inner messages, they can use standard H.248/MEGACO protocol. H.323 or SIP can be used among MG.

4. THE PROCESS OF CALL DEALING WITH SIGNALING

The call dealing process of circuit exchange system includes call clearing and the relating switching and relocation process. Front here take the mobile plat initiates to the load bearing establishment as an example. The analysis call setup process MSC Server principle of work, as well as to moves in the softswitch to call controls the flow to carry on the analysis, emphasized the system realizes the control and the service separation core thought in MSC Server.

(1) MSC Server builds signaling when receives the call sending by the host call mobile plat, after completing the turning on of the control, MSC Server sends the signaling back to the host call mobile plat, at the same time, it starts to send IAM signaling to the next entity. The message of the IAM signaling includes first to load bearing establishment instruction, possible continuously instruction,bearer characteristics and possible media gateway mark.

(2) MSC Server receives the bearer message and signaling of the next point, such as bearer address and binding reference. MSC Server sends increasing endpoints instructions to mobile media gateway by H.248 protocol, and then ask mobile media gateway to build bearing of the directional goal migration media gateway and to connect the latter bearer by using the Change Trough-Connection. Realizes the bearer establishment flow in the migration media gateway

(3) UMTS access to the bearer establishment process: MSC Server sends increasing endpoints instructions to mobile media gateway by H.248 protocol, and asks the mobile media gateway to provide the bearer address binding reference of the input endpoints. It requires Backward Trough-Connection Bearer by using Change Trough-Connection. Though Radio Access Bearer, it assigns requests letter command, informs BNC to initiate the load bearing establishment and Iu UP initialization process.

(4) Access to the bearer establishment process: MSC Server requires the mobile media gateway to remain a TMD circuit by H.248 protocol[2][4], and it requires Backward Trough-Connection Bearer by using Change Trough-Connection. And through after to the assignment request letter command informs the BSC execution to accessed the bearer assignment.

(5) Access to the bearer assignment situation in the early time, if accessed bearer assignment already to complete, MSC Server continuously sends the pitch point instruct command.

(6) After MSC Server accepts address entire message, it sends prompt message to the host mobile plat. After receives the picking machine letter which calls is made, through the H.248 agreement requests the migration media gateway bidirectional connects the bearer, and request input end point and output end point activation inter working function and pronunciation processing function.

5. ROUTING SELECTION

Regarding each call, usually defers to the priority hypothesis on many routes, for selects the most superior route, in this system CDC selects two routing methods: the overflow type and the load shares type[5][9], these two methods all are in the correspondence commonly used to choose the road strategy.

The overflow type chooses the road according to each route's priority, after first route is entire busy again, then chooses the priority low route. This principle request from goes directly route to start to consider each route and check if they do satisfy the following three conditions:

1) This route corresponds DPC to be possible to reach and also the users may partial be used.
2) Chooses CS in this route, this route corresponds in CS exists idle electric circuit.
3) The route corresponds DPC will not congestion.

If exits route satisfies above three conditions, then chooses the road to succeed and to obtain the corresponding route and CS, otherwise chooses the road defeat. Next we will show how overflow type chooses the road.

When CS receives the call dealing request, first obtains the direction the multi- strip route through the number analysis, then CS will send the route information to issue CDC by call choosing road request. After CDC receives the message, judges the choosing road way is the overflow type, and then choose route and CS according to the follow process. Detailed flow like Figure2. shows and each step concrete operation is as follows:

1) Determine several called certain direction routes according to the route information, and choose current router as the directly router, then starts from the current router to choose the road.
2) Judges whether also has may choose the router, if, then enters step 3, otherwise routing fail.
3) Inspects the choice of the router corresponding DPC whether can't reach or the user part cannot use, if, then takes the next router as the current router, returns to step 2 and choose the next router as the current router, otherwise enters the next step 4.
4) Inspects the choice of the router whether entire corresponding CS to be busy, if, then takes the next router as the current router, returns to step 2 and choose the next router as the current road. Otherwise, the selection has the idle electric circuit CS, enters the next step 5.
5) Inspects the choice of the route DPC corresponding whether jams, if, then takes the next router as the current router, returns to step 2 and choose the next router as the current road. Otherwise, add 1 to the congestion counter, increase a level to the congestion condition corresponding this route, choose the routing success.

We gives an example to describe this flow simply, supposes some character crown correspondence to have two routes, respectively named route 1 and route 2, route 1 is the directly arrived router. Route 2 is the first circuitous route. When chooses the road, first chooses route 1, if the route 1 corresponds DPC not to be possible to reach or the user part cannot use, then chooses route 2. Otherwise, chooses road in turns in mechanism in route 1 which corresponds CS, if CS entire busy, chooses route 2. Otherwise, inspects route 1 corresponding DPC whether congestion, if congestion chooses route 2, otherwise routing success.

The load shares type for choosing road shares the telephone traffic in each route by the different load proportion, establishes a route wheel counter for this, when achieved the load shares proportion, choose the next route. It must support completely load route in the load shares type, namely according to overflow type to choose one or several optimal routes, and choose other routes according to the load shares type. Also it should support the route to be hot spare, namely according to overflow type to choose some routes, chooses the hot spare route only after all electric circuits of these routes completely to be elected. For example, we can take the directly arrived route as the full load route, chooses the circuitous route according to load shares type when the directly arrived route is busy entirely. The load shares type requests to start from the current route according to following three rules to consider in turn each route until routing success when it chooses the road:

1) If exists full load type route, then the overflow type chooses the full load type route.
2) Chooses a non-hot backup route according to the load shares ratio.
3) If exists the hot backup route, then the overflow type chooses the hot backup route.

Explains the application examples about the route round of elections counter as follows. Supposes some character crown correspondence to have two routes, respectively named route 1 and route 2, the load shares ratio is 3 and 5. Then in the call process, first calls 3 times in the route 1, then calls 5 times in the route 2, then calls 3 times again in the route 1, analogizes in turn. In this process, uses the route round of elections counter to record the number of calls which already carried in the current route.

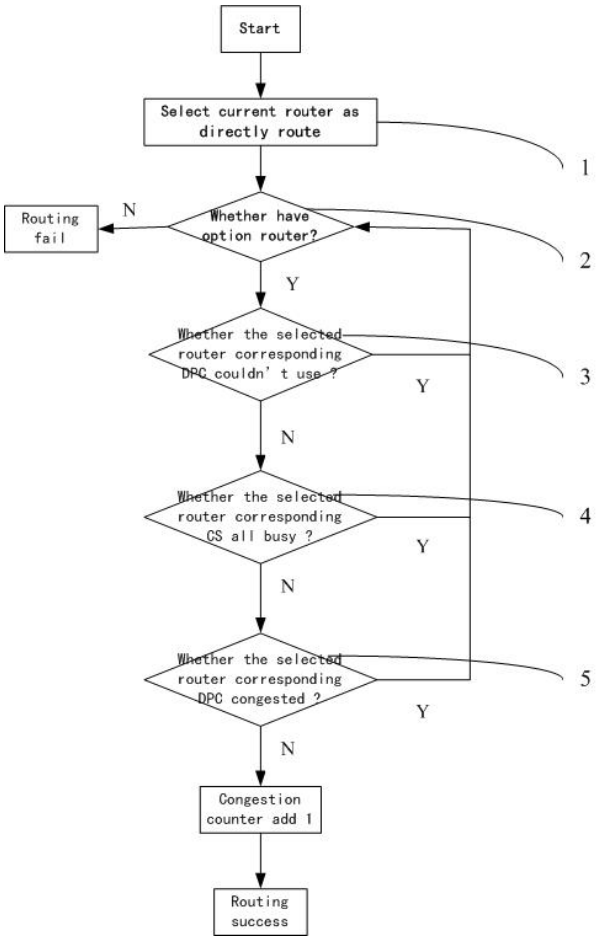


Fig.2. Overflowed call routing

6. CONCLUSIONS

The connection of softswitch technology and the mobile communication technology has the huge superiority, and it already became the study hot point of NGN. This paper proposes a call model based on the distributed MSC-Server which is in the foundation of the mobile softswitch technology, and made the detailed research and the analysis to its call process of the signaling flow. Along with each kind of new service as well as the increment service unceasing increase and the request unceasing enhancement, the original MSC call controls becomes more and more complex. This distributed MSC-Server proposed singaling controlled by CDC, CS and SG, the electric circuit state management, service receiving and dispatching and the transmission are realized by the MG in this paper, it can makes the call control be independent to the bottom floor bearer protocol. Realizes the design requests of the mobilized call control in the softswitch.

REFERENCES

[1] Josef Glasmann,Wolfgang Kellerer,Haraled Muller. Service Architectures in H.323 and SIP: A Comparison. IEEECommunicationsSurveys&Tutorials[J].2003.

[2] RFC3525:*GatewayControlProtocol ersion*[S] ,2003.

[3] IETF RFC2705: *Media Gateway Control Protocol (M GCP) Version 1.0* [S] 1999.

[4] ITU – T H. 248 Gateway control protocol[S] ,2000.

[5] International Softswitch Consortium,*Reference Architecture Version 1.2*http://www.isc.org.

[6] Ohrman JR F D. *Softswitch Technique*[M]. Electronics industry Press, 2003.

[7] Chen jian ya，Yu hao. *Softswitch and Ngn*[M]. Beijing University of Posts and Telecommunications Press, 2003.

[8] The Parlay Group. Parlay API Specification. http://www.parlay.org.

[9] Rita Puzmanova. Router and Switch[M]. POSTS & TELECOM PRESS, 2004.

A Method of Analyzing the Reliability of Distributed Communication Network Management System

Weizhan Han, Sidong Zhang, Yu Sun
School of Electronics and Information Engineering, Beijing Jiaotong University
Beijing 100044, China
Email: hwzhwz6409@sohu.com

ABSTRACT

The distributed network management system (NMS, the same hereinafter) is an important supporting system for a communication network. So we should pay more attention to its reliability. In reliability research filed of communication network, especially in project design, the reliability study on its distributed NMS is becoming a hotspot issue. The traditional reliability research before aimed mainly at the hardware of single equipment and a suit of perfect method has been put forward. But the study on system or network (consist of many equipments in general) is not enough and the study on software system is less too.

A study on the reliability of distributed NMS which is typical a software and hardware integrated system is performed in this paper and a flowchart of integrated analysis is described. Based on the failure criterion, this paper establishes the reliability model. In the end, the process of this software_hardware system reliability integrated analysis is given and an example is present.

Keywords: Network Management System (NMS), Network Management Subsystem (NMSS), Network Management Center (NMC), Integrated Reliability, Analytic Hierarchy Process Method

1. INTRODUCTION

The distributed NMS is an important supporting system for a communication network. In communication network reliability research filed, especially in project design, the reliability study on its distributed NMS is becoming a hotspot issue. Nowadays, the design and establishment of the NMS of a communication network mostly follow the thought of TMN (Telecommunication Management Network); the NMS often appears with an appearance of a distributed network of management, so the study on reliability of NMS of a communication network is indeed the study on reliability of this distributed network of management.

The study on reliability in the past is often carried on to the hardware of single equipment and there are a set of comparative perfect index systems. The reliability study on communication network is started in the sixties and not to be paid attention until the seventies. Because the reliability study on communication network is a complicated subject in extensive range, no acknowledged standard has been formed until now. According to a large amount of existing documents and materials, the study on reliability of communication network is often made as follow procedure: abstracting communication network into a flowchart which consist of nodes and links and transmit different information，using the mathematics model , setting up or choose different indexes to study with different views. Many achievements have been made already. But these studies are mostly macroscopically, the detail about equipment of communication network and software reliability is seldom considered. It is nearly the blank also about the study on the reliability of the distributed NMS of communication network.

In reliability study on the software, with the gradual enlargement of software function, project able and maximization in software development, the software system is becoming more complicated too; therefore the requisition for reliability of the software is increased further. Most of reliability model of software are supposed according to certain model at present, adopt the methods of mathematical statistics to estimate about the reliability of the software in case of obtaining certain precondition. It has the advantage of clearer mathematics expression, easy to use in software development and planning [1]. But because of the variety of software development ways and the appearance of means and some problems of the model itself, although there are already more than one hundred software reliability models since 1972 when the first software reliability model appearing , no one model can adapt to various kinds of occasion. So far, the study on the software reliability is still very unripe, at theoretical research and exploring stage, and there is a large difference to the actual project. Up to now, no one feasible method can be used to evaluate project software reliability quantitatively yet. The same to distributed NMS of communication network (a typical software system).

So this article, while studying the distributed NMS reliability of communication network, on the basis of reliability conception of the tradition, have fully considered the following systematic characteristic: Firstly, the NMS is a distributed management network consisted of a lot of network management centers (NMCs, the same hereinafter), so, the reliability of NMC and even the whole NMS should be studied from the hardware view, based on single equipment reliability. Secondly, the distributed NMS of communication network is the system that works on the hardware platform, is supported by the software. The software is a main component of NMS; its reliability plays an important role in the NMS. So it is important to study the reliability of its software system. Thirdly, it is important to study the reliability of distributed NMS of communication network which is an integrated system composed of hardware and software. This article aims at proposing one method used to study the reliability from systematic view of distributed NMS of communication network which is an integrated system composed of hardware and software.

2. RELIABILITY ANALYSIS OF DISTRIBUTED NMS IN A COMMUNICATION NETWORK

Nowadays, with the enlargement of the scale of communication network and the adoption of the advanced network management skill system, the system structure of the NMS of communication network mostly follow the thought of TMN , and usually adopt the multilevel, distributed management mode

[2] [3]. Under this mode, the first level NMC is generally set up at highest level, because of itsimportance, usually be allocated according to master—slave manner, to form first level network management subsystem (NMSS, the same hereinafter); several second level NMCs are generally set up at higher level, to form second level NMSS; the rest may be deduced by analogy, several lowest level NMCs are set up in every network node finally, to form lowest level NMSS; The NMC of higher level is manager, the adjoining subordinate NMC is agent. Figure 1 is an example of a three_level NMS, among them, the first level NMC presents the master_slave manner, there are m second level NMCs, and there are n third level NMCs. Because the NMS is a complicated system, there are a lot of factors influencing its reliability, so in the analysis of reliability of the NMS, the invalid criterions of each NMC , the NMSSs at all levels , the whole NMS should be set up at first according to the concrete conditions of system, after that, to set up various kinds of corresponding reliability models on this basis, then to divide each NMC into two major parts: the hardware and the software using the analytic hierarchy process method [4]，to ask out the reliability of the hardware and software respectively and the reliability of each NMC can be obtained by integrating hardware and software reliability, finally , from bottom to top , can get the reliability of each NMSS, the whole NMS respectively.

2.1 NMS Reliability Definition

The reliability of NMS, NMSS at all levels and every NMC can be defined as follow: the possibility that the NMS, NMSS at all levels and every NMC can fully complete stipulate functions within time and condition that users stipulate.

"Stipulate condition" usually means the environmental condition and service condition; "stipulate time" generally refers to the task running time; "Stipulate function" generally involves five function fields: configuration management, performance management, fault management, account management and security management.

2.2 Invalid Criterion

On the basis of the reliability defined and from reliability view, careful analysis should be made to actual operation law and actual function requirement of the system, and then obtain the invalid criterion of the system. To different system structure and different requirement for use of NMS, its invalid criterion may be different.

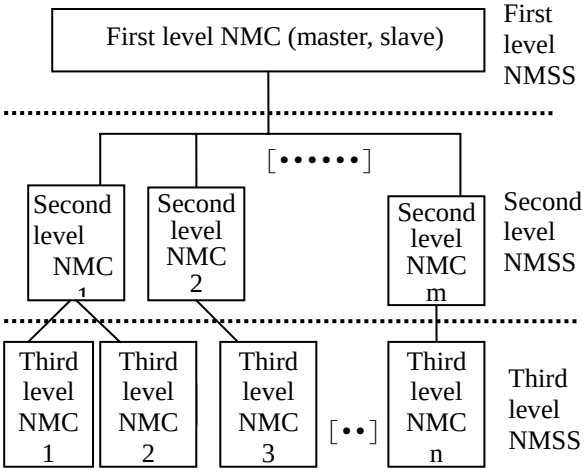


Fig.1. A three_level NMS structure sketch

1) Invalid criterion of the whole NMS

To the distributed NMS of communication network, two kinds of typical invalid criteria are put forward here, it can be chosen according to the actual conditions.

① the first kind of invalid criterion:
Any NMSS at all levels breaking down will bring the whole NMS to lose efficiency, only when every NMSS works normally, the NMS could work normally.

② the second kind of invalid criterion:
In the NMSSs at all levels, when one NMSS breaks down, only some functions of the NMS are influenced , it will not cause the whole NMS to lose efficiency.

2) The invalid criterion of the NMSS at all levels

The invalid criterion is different if it is different to the concrete conditions, functions of the NMSS. Here give a typical invalid criterion of systems (Suppose that the NMS is made up of k level subsystems here):

① to the first level NMSS, when both two first level NMCs(master, slave) in hot-backup state break down, judge that the first level NMSS loses efficiency.

② to i*th* level (i =2, 3…k) NMSS, when one NMC among them break down, according to the system design generally, its management area can be managed by other same or higher level NMC. So when more than ($m_i - n_i$) NMCs break down, we may think this level NMSS lose efficiency. m_i is the quantity of NMCs in i*th* level NMSS, n_i is the lower limit quantity of NMCs which can guarantee the i*th* level NMSS to be in normal working state.

3) The Invalid criterion of every NMC

The NMS is one system that works on the hardware platform, supported by the software, according to the characteristics of different systems, two kinds of invalid criteria of a NMC can be obtained:

① Either the software or the hardware losing efficiency will cause the NMC lose efficiency;

② When software or hardware breaking down, the normal running of NMC is influenced with certain probability.

2.3 Set Up Reliability Model [5]

1) The reliability model of whole NMS

According to the invalid criterion of the whole system, choose the corresponding reliability model as follows:

①By the first kind of invalid criterion, select the series model, obtain the reliability model of the whole NMS:

$$R(t) = R_{1th}(t) * R_{2th}(t) * R_{3th}(t) * \cdots * R_{kth}(t) \quad (1)$$

② By the second kind of invalid criterion, select parallel_in_weight model, obtain the reliability model of the whole NMS:

$$R(t) = \omega_1 R_{1th}(t) + \omega_2 R_{2th}(t) + \cdots + \omega_k R_{kth}(t) \quad (2)$$

in the equation $R_{1th}(t)$, $R_{2th}(t), \cdots R_{kth}(t)$ represent respectively the reliability that first level NMSS , second level NMSS and k*th* level NMSS; ω_1 , ω_2 , $\cdots \omega_k$ represent corresponding weight coefficients respectively, can be obtained with experts judge method[6] .

2) The reliability model of NMSS at all levels

According to the invalid criterion of NMSS too, the reliability model of every NMSS can be obtained as follows:

①First level NMSS is configured with master and slave, so we can select model of parallel heat-backup of two units:

$$R_{1th}(t) = \frac{s_1}{s_1 - s_2}\exp(s_2 t) - \frac{s_2}{s_1 - s_2}\exp(s_1 t) \quad (3)$$

In the equation:

$$s_1, s_2 = \frac{1}{2}[-(3\lambda + \mu) \pm \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}]$$

λ is the lose efficiency rate, μ is the repairing rate.

②The i*th* level (i =2.3 ...k) NMSS is made up of m_i NMCs, according to the invalid criterion, we can select "n_i from m_i "vote and redundant model:

$$R_{ith}(t) = \sum_{j=n_i}^{m_i} C_{m_i}^{j} R_{ict}^{j}(t)[1 - R_{ict}(t)]^{m_i - j} \quad (4)$$

in the equation, $R_{ict}(t)$ express the reliability of an i*th* level NMC;

3) The reliability model of every NMC

According to the invalid criterion of the every NMC, select series model or parallel_in_weight model respectively, we can obtain its reliability:

$$R_{sys}(t) = R_S(t) * R_H(t) \quad or$$

$$R_{sys}(t) = \omega_1 R_S(t) + \omega_2 R_H(t) \quad (5)$$

in the equation, $R_{sys}(t)$ express the reliability of a NMC, $R_S(t)$ show the reliability of the software system, $R_H(t)$ show the reliability of the hardware system. ω_1, ω_2 express software and hardware system weight coefficient respectively, can be obtained by expert's judge method.

2.4 Find the Reliability

After the reliability models are set up, the reliability can be obtained. Solve the reliability of every NMC at first, and then get the reliability of NMSS at all levels and the whole NMS respectively according to the reliability models at all levels.

1) Reliability of single NMC

Use analytic hierarchy process method; divide the NMC according to its component into levels. The method to divide can be chosen concretely according to the situation of the concrete system, a kind of comparative typical method is provided here, shown as Figure 2.

① the reliability of the hardware system

Divide the hardware of the NMC according to the equipment component into the module such as server, customer machine, network equipment, power supply unit, etc. (different systems can be divided according to different concrete conditions). Series model and parallel_in_weight model can be selected according to the invalid criterion of the system and function requirement. Suppose that reliability of every module is: $R_1(t)$, $R_2(t)$, $R_3(t)$, $R_4(t)$, $R_5(t)$, $\cdots$, $R_n(t)$, they can generally be obtained from the given reliability index of every equipment.

In case of series model, the reliability of the hardware system can be obtained as follow:

$$R_H(t) = R_1(t) * R_2(t) * R_3(t) * R_4(t) * R_5(t) * \cdots * R_n(t)$$

In case of parallel_in_weight model, the reliability of the hardware system can be obtained:

$$R_H(t) = \omega_1 R_1(t) + \omega_2 R_2(t) + \omega_3 R_3(t) + \cdots + \omega_n R_n(t)$$

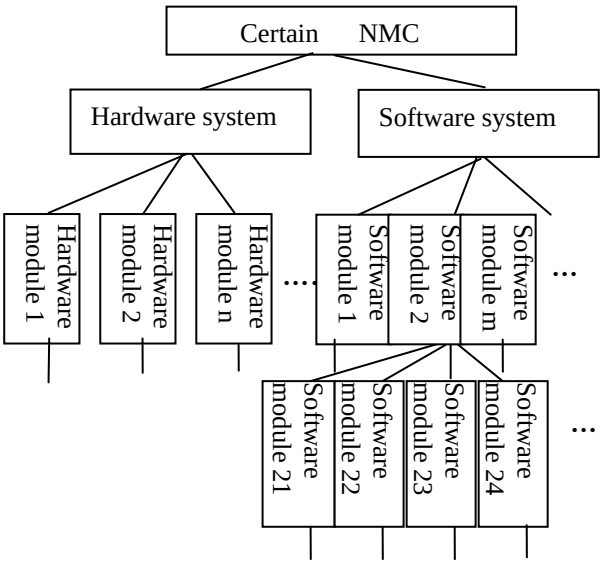


Fig.2. Multi-level software_hardware module of NMC

among them $\sum_{i=1}^{n} \omega_i = 1$. The weight coefficients can be obtained from the Saaty 1-9 graduation method described in the analytic hierarchy process method.

② the reliability of the software system

The traditional software reliability models are all supposed on the basis of certain probability, not suitable for analyzing the reliability of the project software. And the network management software of communication network is a kind of large-scale project software, and adopts module design generally. So it is a good choice to adopt the module analysis method [7] to solve reliability of the network management software.

The module analysis method divides the software into modules according to the natural structure and function characteristic of the software, then modeling on the level of the module. Its reliability model is:

$$R(t) = 1 - c * b * d * \int_t^{\infty} \int_0^1 e^{-zx^a} dx\, dt \quad (6)$$

In the equation: $z_i = (a_i + 1) * b_i t_i$, t is task running time;

a_i is the processing distribution of the module i. b_i means the possibility of invalid incident happening while running module i. depend on the data input condition mainly. c_i is the capacity of defect of the module i. d_i shows the probability that the module is transferred while the software operates[8][9][10] .

According to the software module division in Figure.2, we can ask for the reliability of every software module in lowest level using Eq.(6). For the concrete module, the parameter of models should be confirmed according to the rule needed to confirm parameter of the model. Then choose the reliability model to superpose to get the

reliability of the intermediate level module according to the invalid criterion, upwards step by step, we can get the reliability of whole software system $R_S(t)$ finally.

③integrated reliability of software and hardware of a NMC

After getting the reliability of the software, hardware system, according to systematic function analysis, choose the corresponding reliability model, we can get the reliability of a NMC synthetically by using Eq. (5).

2) Reliability of the NMSS at all levels and whole NMS

After getting the reliability of a NMC, we can get the reliability of first level, second level and subordinate NMSS: $R_{1th}(t)$, $R_{2th}(t), \cdots R_{kth}(t)$ by using Eq.(3), Eq.(4). Finally, we can get the reliability of whole NMS $R(t)$ by using Eq.(1), Eq.(2).

3. INSTANCE ANALYSIS

3.1 Instance Backgrounds

Certain project is a three_level distributed NMS, among them the first level NMC is allocated according to the master and slave manner, second levels NMC have 10, third levels NMC have 30. All the software design is according to the module thought.

According to the systematic reliability requirement, whole system's mean time between failures (MTBF) is no less than 2000 hours. The mean time to repair (MTTR) the hardware equipment is no more than 30 minutes .in the typical work pattern, the systematic task duration is no less than 336 hours.

3.2 Select the Reliability Models and Divide System

According to the whole system's application characteristic, the reliability of the whole NMS adopt parallel_in_weight model; First level NMSS's reliability adopt parallel heat_backup of two units model; second and third NMSS's reliability adopt "n_i from m_i "vote and redundant model; NMC adopt series model; The hardware or software of a NMC adopt parallel_in_weight model .

The division of software and hardware module of every NMC is shown as Fig.2. The equipments of each NMC at all levels are same on the quantity and category basically, only the hardware configuration and software complexity are simplified gradually from top to bottom levels.

3.3 Reliability Calculation

1) The hardware reliability of the first level NMC

The life of the hardware equipment generally obeys the of negative index distribution, the equation of getting its reliability is: $R(t) = \exp(-\lambda t)$

among them, λ is the losing efficiency rate of the hardware equipment, t is task running time. Suppose the reliability of network equipment, power supply unit and computer is $R_{Y1}(t), R_{Y2}(t), R_{Y3}(t)$ respectively, using parallel_in_weight model and superposing the reliability, the reliability of the hardware system of the first level NMC can be obtained as follow:

$$R_{1H}(t) = \omega_1 R_{Y1}(t) + \omega_2 R_{Y2}(t) + \omega_3 R_{Y3}(t) = \omega_1 e^{-\lambda_1 t} + \omega_2 e^{-\lambda_2 t} + \omega_3 e^{-\lambda_3 t}$$

among them: -- t is systematic task running time, here 336 hours.

-- λ_1, λ_2, λ_3 is the losing efficiency rate of network equipment, power supply unit and computer respectively. According to the character of negative index distribution, losing efficiency rate and mean time between failures (MTBF) are reciprocal. According to the technical parameters of purchased equipments, the MTBF of the network equipment, power supply unit and computer is 10000 hours, 5000 hours and 5000 hours respectively.

-- ω_1, ω_2, ω_3 is the weight coefficient of network equipment, power supply unit and computer respectively. They are confirmed as 0.2, 0.2 and 0.6 through Saaty 1-9 graduation method.

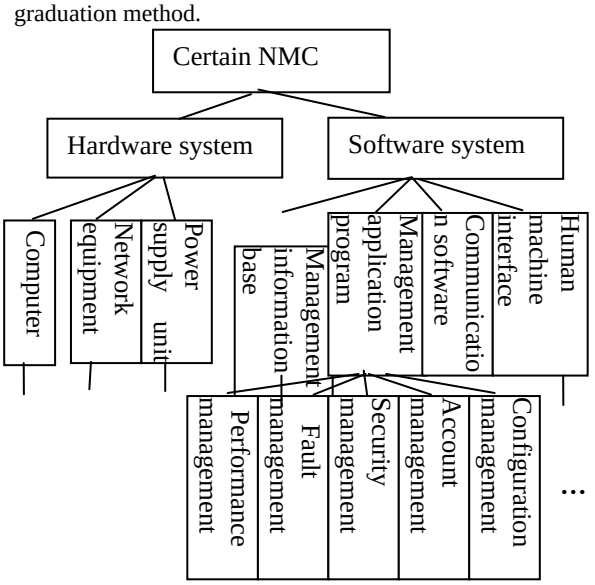


Fig.3. Division of hardware and software module of NMC

The hardware reliability of the first level NMC can be calculated as 0.936.

2) The software reliability of the first level NMC

at the lowest level , regard fault management module as the example , according to the concrete characteristic of the module in this NMS, through analyzing, the model parameters of this module can be obtained as follow: a_i =10, b_i =0.00000048, c_i =80, d_i =0.3, module running time is 20160 minutes (336 hours), the reliability of this software module can be calculated as 0.738 .

The reliabilities of performance manage module, security management module, configuration management module and account management module can be obtained in same way. Use Saaty 1-9 graduation method to distribute corresponding weight coefficients for each software module at the same time, the reliability of management application program module in upper layer can be obtained as 0.752 by selecting parallel_in_weight model. The concrete number value is shown in the following table 1.

In the same way, the reliability of management information base, communication software, human-machine interface module can be obtained as follows: 0.803, 0.657, and 0.785. The reliability of software system can be obtained as 0.742 by selecting parallel_in_weight model and distributing corresponding weight coefficients. The concrete number value is shown in the following table 2.

Table 1 Reliability of the management application program

Module name	Fault management	Performance management	Security management	Configuration management	Account management
Reliability	0.738	0.857	0.835	0.718	0.707
Weight coefficient	0.333	0.111	0.112	0.333	0.111
Reliability of the management application program module：0.738* 0.333+ 0.857* 0.111+ 0.835* 0.112+ 0.718* 0.333+ 0.707* 0.111 =0.752					

Table 2 Reliability of software system

Module name	Management information base	Management application program	communication software	human-machine interface
Reliability	0.803	0.752	0.657	0.785
Weight coefficient	0.200	0.250	0.300	0.250
Reliability of software system：0803* 0.200+ 0.752* 0.250+ 0.657* 0.300+ 0.785* 0.250 =0.742				

3) The reliability of first level NMC
The reliability of first level NMC is 0.742*0.936=0.695 by selecting series model.

4) The reliability of first level NMSS
The parallel heat-backup of two unit's model is adopted to ask for the reliability of the first level NMSS, its reliability is 0.898 by using Eq.(3).

5) The reliability of whole NMS
According to reliability computing method mentioned above, the reliability of second and third level NMSS can be obtained respectively in the same way; the reliability of whole NMS can be obtained by selecting parallel_in_weight model and distributing corresponding weight coefficients with expert judge method. The concrete number value is shown in the following table 3.

Table 3 Reliability of the whole NMS

System name	Reliability	Weight coefficients
First level NMSS	0.898	0.5
Second level NMSS	0.817	0.35
Third level NMSS	0.813	0.15
Reliability of the whole NMS: 0.898* 0.5+ 0.817* 0.35+ 0.813* 0.15 =0.857		

6) Result analyzed

① Through reliability calculation mentioned above, the reliability of this three_ level NMS is 0.857, changing this reliability into the network mean time

② According to the assessment experience of a lot of projects in the past, the MTBF of three_level NMS with the same scale and equal application occasion is generally between 2000-2400. So the assessment result using this method is in the rational scope.

③ If the traditional method is adopted and use reliability of the hardware system as the reliability of the whole NMS, the reliability of NMS is 0.936 by calculation. It is obvious that the result obtained by adopting the integrated assessment method of the software and hardware is stricter than the result obtained only by adopting the reliability of the hardware; this is accord with the actual conditions.

④ This method and assessment result have already been recognized by users.

4. CONCLUSIONS

This paper studies the reliability analytical method of the distributed NMS which is typical software and hardware integrated system. The reliability model of solving the integrated system of software and hardware is given. With the complexity of the distributed NMS of communication network higher and higher, different systems each have one's own characteristic and requirement for use. So, it is more important to choose invalid criterion and reliability model when studying the reliability of distributed NMS of communication system which is typical a integrated system with software and hardware. In addition, the accuracy of choosing them is more difficult to master and the integration reliability of the software and hardware is a difficult point to study too. This article only provides a kind of solution; further research still needs.

REFERENCES

[1] A.Csenki.Bayes,"Predictive Analysis Of a Fundamental Software Reliability Model"[J],*IEEE Trans. Rel,* Vol.39No.2,pp.177-183,Jun,1999.

[2] Yang jia hai,Ren xian kun,*Network Management Theory and Implement Technology [M]*,Beijing, Qinghua University Press,Sep,2000.

[3] Wang xong ying,Han wei zhan,*Communication Network Management Technology [M*],Beijing, National Defence Industry Press,Jan,2003.

[4] Saaty T L,"The Analytic Hierarchy Process"[J],New York,McGraw-Hill,Inc.,1980.

[5] Ding ding hao,*Reliability and Maintainability Project*[M],Beijing ,Electronic Industry Press,1985.

[6] Li hong xing,etc,*Project Fuzzy Mathematics Method and Application* [M],Tianjin,Science and Technology Press ,1993.

[7] Zhang ji xu,Wang qi,"Module Analysis Method of Software Reliability"[J],*Tactics Missile Technology,* 2000.

[8] Everett W W,"Software Component Reliability Analysis"[J],IEEE,1999.

[9] Musa J D,Iannion A,Okumoto K,"Software Reliability" Mesurement,Prediction,Application[J],McGraw Hill, 1987.

[10] He guo wei, Wang wei, *Software Reliability* [M],Beijing,National Defence Industry Press,1998.

A QoS Routing Algorithm for Wireless Multimedia Sensor Networks*

Zongwu Ke [1,2], Layuan Li [1], Nianshen Chen [1,2]
[1] School of Computer Science, Wuhan University of Technology, Wuhan 430063, China
[2] Department of Computer Science, Hubei Normal University, Huanshi 435002, China
Email: kezongwu@163.com

ABSTRACT

The application of low-cost CMOS cameras and microphones and the requirement of more information like image and video and sound has conduced the development of wireless multimedia sensor networks. Because there are several main peculiarities such as resource constraints, variable channel capacity that make QoS routing in wireless multimedia sensor network more challenging. In this paper we compare some existing ant routing algorithm used in wireless sensor networks, and propose a QoS based geographic location aware ant routing algorithm. The simulation indicates that our algorithm is efficient.

Keywords: Wireless Sensor Network, Multimedia, QoS, and Ant Colony Algorithm

1. INTRODUCTION

Recently, with the technologies of multimedia sensors and embedded processors development, the research of Wireless Multimedia Sensor Networks (WMSNs) [1]has been a gradual increase. Because multimedia data can often provide a wealth of information about surroundings of a network, wireless multimedia sensor networks can enhance the traditional sensor network applications and enable several new applications. For examples, the applications for military intelligence, surveillance, and reconnaissance [2] and smart home care and target tracking [3] are researched. In these applications in addition to end-to-end delay and bandwidth, more performance metrics, such as delay jitter and packet loss ratio must be considered by communication protocols.

We will focus on QoS-based routing algorithm for wireless multimedia sensor networks using ant colony algorithm. Exiting work on ant routing for wireless sensor networks such as [4]and [5] only consider the energy cost and lifetime of networks, but do not address the multi-constrained QoS guarantees. In this paper the multi metrics such as energy, bandwidth, and delay are considered in an ant routing for wireless multimedia sensor network. The QoS-based routing for wireless multimedia sensor network has great challenging because of some peculiarities [1]. For example the resource constraints, variable channel capacity, etc. So research on the QoS-based routing must be constrained by lack of global knowledge, reduced energy, and computational ability of the individual nodes in WMSNs. An efficient routing algorithm for wireless multimedia sensor network must meet some basic requirement: (1) the nodes memory must reduce; (2) the convergent speed must be quick; (3) the multi QoS constrains must be considered.

Recently some QoS provisioning protocols for wireless sensor network have been proposed, the typical protocol is SPEED[6]. It is designed to provide soft end-to-end deadline guarantees for real-time applications using a geographic forwarding mechanism. MMSPEED [3] is an significant extension over SPEED, which can efficient differentiate between flows with different delay and reliability requirement. But they are not fit the non real-time application in wireless multimedia sensor network, and they provide a probabilistic QoS guarantee not an optimal algorithm.

In this paper we propose a geographic aware ant routing to provide end-to-end QoS guarantee for wireless multimedia sensor networks. The simulation indicates that our algorithm is efficient.

2. RELATED WORKS

The characteristics of the ant colony algorithm, for example, local information required only, positive feedback, distributed computation, and constructive greediness, seem to fit the QoS-based routing problem of wireless multimedia sensor network very well. Various ant-based routing algorithm have also been proposed for wireless sensor network [4;5;7-9]. In reference [4], an energy efficient ant-based routing algorithm was proposed. The energy of nodes used to find next hop, and each node only keeps record of each ant that was received and sent to reduce the memory used. In reference [5], the main goal is to maximum the lifetime of network while discovering the shortest paths using basic ant colony optimization. In reference [7], a Queen-Ant-Aware-Based algorithm was proposed for wireless sensor network. It used GPS to get the position information, and compartment the region. In reference [9], first implement a basic ant routing which did not perform well because of the properties of highly dynamic nodes and asymmetric links in sensor network, then developed three improved versions of ant routing based on the message-initiated constraint-based routing framework: the Sensor-driven and cost-aware ant routing (SC), Flooded forward ant routing (FF) and Flooded piggybacked ant routing (FP). In SC assume that ants can smell where the food is even at the beginning to solve the problem of the forward ant normally take a long time to find the destination (we called initial problem). In FF, a flooded forward ant routing was used to find destination. In FP, a constrained flooding was used when data transmitted to find good paths at the same time to solve high loss rates problem. In reference [8], a ACO-QoSR algorithm was presented, ant it used end to end delay constraints to update pheromone.

In table 1, we compared the algorithms all of above. Obviously, they are not comfortable to the wireless multimedia sensor network very well.

3. PROBLEM FORMULATION

In this paper we discuss the end-to-end multi-constrains QoS routing in wireless multimedia sensor network. Our goal is to

* This work is supported by the National Natural Science Foundation of China under Grant No.60672137, the Specialized Research Fund for the Doctoral Program of Higher Education of China (20060497015) and the Grand Research Project of Hubei Province Department of Education in China under Grant NO. D200622003.

find an optimal routing satisfying the necessary QoS parameters. We assume each node aware its geographical location using GPS or distributed location service in our research. The network model is defined as follow:

Table 1. The comparison of some existed ant-based routing for wireless sensor network.

Algorithms	Initial problem	Memory require	QoS parameters
Reference 3	Not consider	small	Residual energy only
Reference 4	Not consider	more	Residual energy only
Reference 5	Not consider	more	Residual energy only
Reference 6	Assume solved	more	Using multi path to reduce loss rates
Reference 7	Not consider	more	Energy and delay
Reference 9	consider	small	Not consider

The network is represented by a graph $G=(V,E)$ where V is the set of nodes and E is the set of duplex links between the node-pares. Each node $v \in V$ has a transmission range r. Let $d(v_1,v_2)$ be the distance between two nodes $v_1,v_2 \in V$. An edge $e(v_1,v_2) \in E$ between two nodes $v_1,v_2 \in V$ exists if $d(v_1,v_2) \le r$.

The purpose our algorithm is to find an optimal routing providing QoS guarantee such that:

(1) The bandwidth requirement is guaranteed.
(2) The end-to-end delay requirement is satisfied.
(3) Maximum the lifetime of network.

The problem can be defined as follows:

Given a graph $G=(V,E)$, a source $s \in V$ and a sink node $d \in V$, find a route P that following condition are satisfied:

(1) $bandwidth\ (P) \ge B_{\min}$, $B_{\min}$ is the bandwidth requirement;

(2) $delay\ (P) \le D_{\max}$, $D_{\max}$ is the delay requirement;

(3) Maximum the lifetime of network.

The bandwidth is defined as

$$bandwidth\ (P) = \min\{bandwidth\ (e(v_i,v_j)), e(v_i,v_j) \in P\}.$$

The delay is defined as

$$delay\ (P) = \sum_{e(v_i,v_j) \in P} delay\ (e(v_i,v_j)).$$

4. LOCATION AWARE FORWARD ANT ROUTING

4.1 Basic Ant Routing

In order to compare the difference, we first introduce the basic ant routing in reference [9]: Fist forward ant is launched from source node to find the destination node according to the link probability distribution at some intervals, when a forward ant finds the destination, a backward ant is created and move back to the source alone the route which find by the forward ant, in the same time probabilities of nodes in the path are updated according to the evaluation of the path.

The basic ant routing have some disadvantage, for example the initial probability of all the links are equal, that cause the forward ants use a long time to find destination. To improve to performance Zhang propose an initial probability method with cost estimation and local cost function. In this paper we propose a new efficient initial method with QoS guarantee.

4.2 The Define of Geographic Location Aware Forward Ant

We assume the forward ant knows its geographical location, and the location of sink node. The forward and select next hop in the forward neighbor set. The forwarding neighbor set is defined like reference [6].

Define 1. The forwarding neighbor set of node *i* : $FS_i = \{v_i \in NS_i | L - L_{next} > 0\}$, the NS_i is the neighbor set of node *i*. These nodes are inside the cross-hatched shaded area as shown in Fig 1.

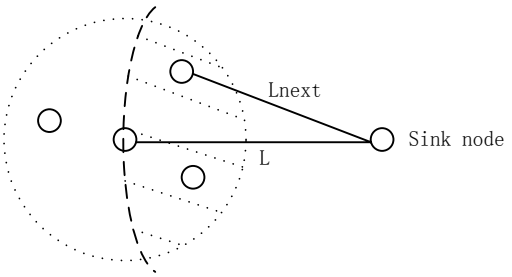


Fig.1. The forward neighbor set of a node

In our routing algorithm nodes only keep a routing table with the probabilistic of each node which belong to forward neighbor set. This method can reduce the memory requirements of nodes. The forward ant select next hop from forward neighbor set and if the sink node is an element of the set, set the probability to 1 directly. This method can solve the problem of the forward ant normally take a long time to find the destination.

4.3 Probability Initial Algorithm

The initial probability of node i to node j calculate with the following formula:

$$p_{ij} = \begin{cases} \dfrac{E_j^{\alpha} \bullet D_j^{\beta}}{\sum_{n \in FS_i} (E_n^{\alpha} \bullet D_n^{\beta})}, & bandwidth\ (e_{ij}) > B_{\min} \\ 0, & bandwidth\ (e_{ij}) < B_{\min} \end{cases} \quad (1)$$

If sink node is a neighbor node of i, set the probability of node i to sink node as 1, else calculate with formula (1). Where E_j is the residual energy of node j, D_j is the delay of edge e_{ij}, $bandwidth(e_{ij})$ is the bandwidth of edge e_{ij}, α and β are constants that determine the relative influence of the energy and delay.

In formula (1), we only use the local information of a node to fit the application of wireless multimedia sensor networks, and provide bandwidth guarantee. At the same time, we use a higher probability to select node which have more residual energy and that can be maximum the lifetime of network. The delay which used of formula (1) is the length of queue in a node. This can reduce the end-to-end delay of the selected path.

4.4 The Forward Ant Routing Algorithm

If a forward ant of a source node arrive node j at first time, the node first calculates its forwarding neighbor set because the set is dynamic in wireless sensor network. Then calculate the probability of all forwarding neighbor according (1) and create a routing table for it. The next hop selected according to probability for the next ants.

5. THE BACKWARD ANT ROUTING ALGORITHM

If a backward ant which is coming from node m arrive node k, the probability of p_{km} is updated according to formula (2).

$$\begin{aligned} p_{km} &= p_{km} + r(1 - p_{km}), \\ p_{kn} &= p_n - rp_{kn}, n \in FS_k \wedge n \neq m \end{aligned} \tag{2}$$

The reward $r \in [0,1]$ is defined as follow:

$$r = \begin{cases} 0, & delay\ (P) > D_{\max} \\ \dfrac{E_m}{\sum_{i \in FS_k} E_i}, & delay\ (P) \le D_{\max} \end{cases} \tag{3}$$

If a path is not providing delay guarantee, the update will not perform. If a path provide delay guarantee, the reward will decide by current residual energy of node.

6. SIMULATION

We simulate our algorithm with MATLAB. In this paper we only discuss the QoS routing algorithm not a real routing protocol, so we perform a program with MATLAB to research the performance of the algorithm. The topology is generated randomly with 100 nodes in area 100×100, and shown in Fig.2. The bandwidth is generated randomly with [1,10], and the delay of each edge is generated with [10,20], and the energy of each node is defined as a constant in the beginner, and energy value reduce 1 if a node is selected once . We first simulate the base ant routing algorithm, the source node is 1, and the destination node is 58, the ant routing algorithm is set like that: the ant number is 10, and the parameter alpha is 1, the parameter beta is 1, the number of iterative is 500, and we use the following formula to evaluate the routes:

$$fit = 1/delay \tag{4}$$

The delay is the total delay of a route.

In Fig 3 we compare the best route and the average fit of routes which find by ten ants. We can find that the base ant routing algorithm is convergence in 80 iterative, and if we reduce the number of ants the convergence time will increase. It indicates that the base ant routing algorithm is not fit to wireless sensor networks because the convergence time is too long, and it use too many resource.

Then we simulate the geographic location aware ant routing algorithm with the parameter like that the ant number is 2, and the parameter alpha is 1, the parameter beta is 1, the number of iterative is 100. The simulate result is shown in Fig.4. It indicate that it is more efficient then the base ant route algorithm.

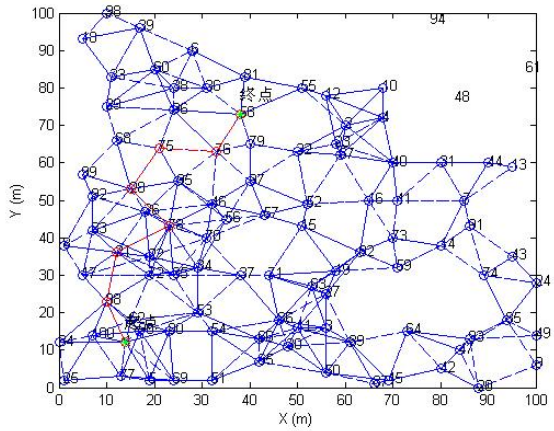


Fig.2. The network topology

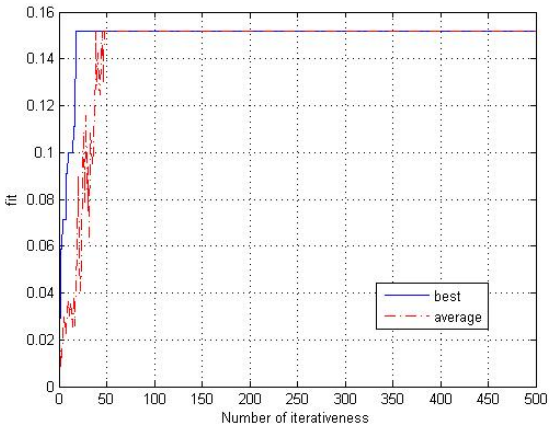


Fig.3. The X axis is the number of iterative; the Y axis is the fit of each route.

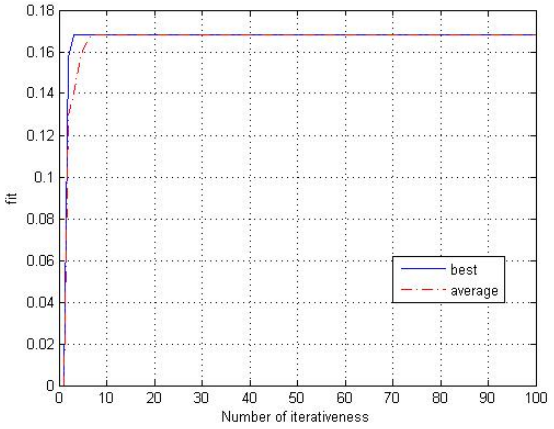


Fig.4. The X axis is the number of iterative; the Y axis is the fit of each route.

7. CONCLUSIONS

In this paper we propose a QoS based geographic location aware ant routing algorithm. Because the ant routing algorithm only used the local information, it needs lesser resource of wireless sensor node, so it seem fit with wireless sensor network, but the base ant routing algorithm because of the

convergence time is too longer. We improvement the performance of ant routing algorithm with the geographic location, and let it can provide QoS guarantee. The simulation indicates the algorithm is efficient. The next research is to design a location aware ant routing protocol and simulated with NS2.

REFERENCES

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks,"in *Computer Networks*,vol. 51,no. 4,pp.921-960,2007.

[2] J. A. DeBardelaben,*Multimedia sensor networks for ISR applications. NEW YORK: IEEE*,2003,pp.2009-2012.

[3] E. Felemban, C. G. Lee, and E. Ekici,"MMSPEED: Multipath Multi-SPEED Protocol for QoS guarantee of reliability and timeliness in wireless sensor networks,"in *IEEE Transactions on Mobile Computing*,vol.5,no.6,pp. 738-753,2006.

[4] T. Camilo, C. Carreto, J. S. Silva, and F. Boavida, *An energy-efficient ant-based routing algorithm for wireless sensor networks*,BERLIN: SPRINGER-VERLAG BERLIN, 2006,pp.49-59.

[5] S. Okdem and D. Karaboga, "Routing in wireless sensor networks using ant colony optimization,"in *First NASA/ESA Conference on Adaptive Hardware and Systems*, pp.4,2006.

[6] T. He, J. A. Stankovic, T. F. Abdelzaher, and C. Lu, "A spatiotemporal communication protocol for wireless sensor networks,"in *Parallel and Distributed Systems*, vol.16,no.10, pp.995-1006,2005.

[7] H. J. Sun, J. Jiang, M. L. Lin, and X. Z. Tan, *Queen-ant-aware-based algorithm for wireless sensor networks routing*. NEW YORK:IEEE,2006,pp.622-626.

[8] C. Wenyu, J. Xinyu, Z. Yu, C. Kangsheng, and W. Rui, "ACO based QoS routing algorithm for wireless sensor networks,"in *Ubiquitous Intelligence and Computing. Third International Conference*, UIC 2006. Proceedings (Lecture Notes in Computer Science Vol. 4159), pp. 419-428, 2006.

[9] Ying Zhang, Lukas D.Kuhn, and Markus P.J.Fromherz, "Improvements on Ant Routing for Sensor Networks," Berlin / Heidelberg: Springer, 2004, pp. 154-165.

Zongwu Ke is an Associate Professor, Department of Computer Science, HuBei Normal University. Moreover, He is Ph.D candidate in Wuhan University of Technology. His research interests are in wireless sensor networks, QoS routing, and protocol engineering.

Worst Case Execution Time Estimate for Real-time System Based on Fuzzy Petri Net*

Yongxian Jin[1], Shuyu Li[1]
[1] Zhejiang Normal University, College of Mathematics, Physics and Information Science, 321004 Jinhua, China
E-mail:jyx@zjnu.cn

ABSTRACT

The results of most worst-case execution time (WCET) estimate method are over pessimistic, and cause great waste of resources if scheduling is based on these results. A new approach for WCET analysis of real-time system software is presented, which is generated from Fuzzy Petri net specifications. The presented approach is a part of our work towards predictability research of real-time system. The whole WCET analysis is divided into three layers, which are fuzzy Petri net modeling, flow analysis and low analysis. The second estimation approach in low analysis is proposed to advances the operation efficiency of processors and decreases the resource waste effectively. The detailed analysis is demonstrated via a case. At last, emulate experiment proves that the presented approach for WCET is more accurate than traditional methodology.

Keywords: Worst Case Execution Time (WCET), Fuzzy Petri net, Real-time System.

1. INTRODUTION

Correctness of output and restriction of runtime are vital characteristics of real-time systems. Real-time scheduling is a mechanism by which hardware and software resources are distributed to real-time system. Proper scheduling makes the real-time system run timely and rightly. Predicting WCET (Worst Case Execution Time) for the system in advance is a precondition of the real-time scheduling and schedulable analysis, and it is also a part of real-time system prediction research. WCET is the longest time when the system runs, i.e. upper limit of runtime. Using the maximal runtime, the system resource (e.g. CPU time and memory assignment) is used well so that real-time scheduling can be achieved. Moreover, in multiprocessor circumstances, the value can be considered in order to choose appropriate processor to execute the task. This avoids waste and promotes the processing power of the system.

It is an important research field to estimate WCET for real-time system. WCET concept is presented by [1] firstly, which discusses some limits imposed on program language to calculate the longest execution time of real-time task. Recently, more and more famous colleges engaged in WCET research, e.g. Florida University, Princeton University, York University and Uppsala University etc. International conference on WCET study is opened annually since 2001. But two aspects are worth researching and improving further. One is that the estimation accuracy of current methods is not high enough. The other is that most of researches pay attention to only one phase of WCET estimation, e.g. flow analysis or low-level analysis. Of cause, some researchers present the whole WCET estimation process. For example, The WCET analysis base on Matlab model is presented by Kirner et al[2]. A special C code with additional annotations for WCET analysis is generated. The generated C code is analyzed by WCET analysis tool to calculate WCET. But above mentioned annotations and low-level analysis work in single blocks and tasks of the program, the whole cooperating performance is not considered, which leads to the lower estimation precision. The approach presented by Erpenbach et al[3,4] works on model layer, i.e. State Chart. Meanwhile, State Chart records the maximum number of state transitions, which occur before the system becomes stable after the external event triggering. All possible state transitions are described in state transition graph. The final WCET is calculated by finding the longest path in the graph. But, when the system is larger and more complicated, it is hard to describe asynchronous behaviors or operations for state transition graph. So the WCET estimation is over pessimistic.

To enhance precision of WCET estimate, Fuzzy Petri net modeling is applied in the paper in order to support complex distributing characteristic, concurrent characteristic and asynchronous characteristic of real-time system. Fuzzy Petri net analysis methods are systemic mathematics and graphics descriptive tool supporting asynchronous and concurrent modeling. So Fuzzy Petri net is used to models to the real-time system. Then Fuzzy Petri net code used in WCET estimation analysis is generated from Fuzzy Petri net layer. Low-level analysis is implemented with respect to Fuzzy Petri net code. Furthermore, the final WCET is calculated rightly.

2. WCET ESTIMATION ANALYSIS

The WCET estimate analysis of real-time system is divided into three phrases: ① Flow analysis. In the phases, program code, for example, the number of loop iterations and "if-else" clauses etc. is analyzed to describe the flow structure of the program. ②Low-level analysis, which estimates the WCET for each basic block of the given program in terms of hardware environment, e.g. the execution time of a instruction and the runtime of each atomic unit of the program. Low-level analysis consists of global analysis and local analysis. The influences on execute time by instruction cache and data cache is studied in the global low-level analysis. Those execute time of hardware affects the runtime of the program is considered in the local low-level analysis, e.g. access speed of memory. ③ WCET calculation, i.e. the final WCET is calculated in terms of above two analyses phases. Nowadays, some approaches for WCET calculation are listed below. First one is based on path (path-

* This work is supported by the Natural Science Foundation of Zhejiang Province #Y104105.

based)[5,6]. All runtime of possible paths are calculated, and the longest one is the WCET estimate. Second one is based on tree (tree-based)[7,8], namely time scheme, which is formalization method to compute WCET. This approach applies rules, which is used to calculate runtime to different program structures, for example, if-then-else etc. This method analyzes source code to reuse rules to compute the longest runtime through traversing syntax tree representing program from bottom to top. The concept of the approach is simple, and its cost is lower. However, it is difficult to deal with the dependence and pertinence of clauses. The last one is based on Implicit Path Enumeration Technique (IPET-based)[9-11]. Algebra and logic specifications are used to express the runtime of program flows and basic blocks, i.e. the program is transformed to a set of IPET specifications. The WCET estimation is calculated by maximal object function meeting the specifications.

3. WCET ESTIMATION ANALYSIS BASED ON FUZZY PETRI NET

3.1 Fuzzy Petri Net Model Applied to Real-time System

Some expressions and analysis methods of fuzzy mathematics are added into standard Petri net, and the extended Petri is named Fuzzy Petri net which can express the behaviors of fuzzy systems. A tuple with seven elements is defined in order to describe the real time and the task execution relationship of the real-time system better: FPN=(P,T,I,O,f,τ,R), P is a finite set of places; T is a finite set of transitions; I is a kind of blurry relation based on P×T, and it indicates connection situation from places to transitions and input connection intensity α. O is another fuzzy relation based on T×P, which indicates connection situation and relevant output connection intensity β. $f(t_i)$is the reliability function, transition t_i is its independent variable. t_i varies among real number range, i.e.$[0,\infty]$, i=1…n; $\tau(t_i)$ is the field function of the transition t_i , t_i varies among real number range, i.e. $[0,\infty]$, i=1…n; $R(t_i)$ is the longest execution time for t_i. The tolerated time is proposed by the real-time system requirements. i=1… n; Fuzzy Petri net can circulate continuously. α, β, τ and f are the vital factors for Fuzzy Petri's behaviors. When f, the reliability function value of t_i, is not less than the field τ, the transition t_i is fired. Then the resource on the input place is decreased, and the output is generated on the output side.

3.2 WCET Estimation Analysis Based on Fuzzy Petri Net

The estimate process base on Fuzzy Petri net is composed by three phases: modeling, flow analysis and low-level analysis.

The modeling to the real-time software is the base of the WCET analysis. During modeling, at first the analysis which modularizes the real-time system is required. The call relationship between modules is achieved. Secondly, according to the relationship, the modeling to the real-time software based on the Fuzzy Petri net is executed, including functional as well as non-functional modules. The details are followed as below.

(1) Analyzing the structure of modules, the call relationship and data flows between modules. The sequential graph describing the call relationship between modules of the whole system is made. Relative resource changes are notated on the graph.

(2) Some information exchanges are added to the sequential graph in terms of the call relationship of modules and utility of the resource, which means to add places and directed edges to the graph. The places and edges are used to express the utility and change of resource during tasks execution. And the tasks are expressed by transitions with field to fire the transitions. At last input and output places are added into the Fuzzy Petri net. Until now, subnets of the whole Fuzzy Petri net are achieved. Then the subnets are linked as the whole Fuzzy Petri Net layer describing the real-time software of the system with respect to the execution sequence between modules. Meanwhile the transitions can be refined. The modeling approach is fulfilled from function and resource distribution. It makes the execution process of the system software clear and understood easily. The following WCET estimation analysis is more systemic and logic.

Flow analysis is the key to WCET estimate. Flow analysis consists of reachability analysis and behaviors analysis. The Fuzzy Petri code is generated in reachability analysis phrase. Additional information is generated in behaviors analysis phrase. The Fuzzy Petri code and behaviors additional information are combined into source code by flow facts language in [12] based on reachability graph. Source code is compiled into object code used by low-level analysis.

Low-level analysis accounts for hardware effect on the execution time, such as, processors and memory. Program blocks are analyzed to calculate the WCET for the event. A method named second estimation is used to improve the accuracy of the WCET estimate. The right processor is selected to run the task through the usage of the second estimation method. To some extent, resource waste is decreased, and the power of the system is enhanced. Figure 1 gives the detailed WCET estimation process.

4. EXAMPLE

The proposed methodology based on the Fuzzy Petri net is explained with the example net in Figure 2. The example net, a small part of air humidifier. In the running process of the model, different events fires different transitions. Furthermore, different response time is obtained. Whether the establishment of the model is good will affect on the accuracy of WCET estimate. The example contains eight places (Event, Wet, Dry, Modest, WetResult, DryResult, ModestResult and Ready) and five transitions (t_1, t_2, t_3, t_4 and t_5). The No. k input connecting intension of transition t_i is marked with α_{ik}, the No. k output connecting intension of transition t_i is marked with β_{ik} .The field of transition t_i is marked with τ_i , The nonnegative reliability function of input intension of transition t_i is marked with f_i , $f_i=\max(\alpha_{i1},\ldots, \alpha_{ik},\ldots, \alpha_{im})$, m is the number of input connectors of t_i. Humidity signals are inputted from the place Event. Then the signals are transformed to digital signals. The digital signals are compared with given references to compute the input connection intensions of transition t_i (i=2, 3, 4) respectively. If the relative value f_i of transition t_i is no less than the field τ_i ($f_i \geqslant \tau_i$), t_i can be fired. The output is generated at the place Ready for other parts calling. The transitions t_2, t_3 and t_4 are can be refined to a subnet base on Fuzzy Petri net.

The purpose of reachability analysis is to generate reachability graph and Fuzzy Petri code in the flow analysis phase. The number of transition iterations is marked on the directed edges of the reachability graph. The number is obtained from transition notations and behaviors analysis [13]. The reachability graph is expressed by Fuzzy Petri code. Then behaviors analysis is imposed on the graph to find the longest path at run-time and execution time of each transition fired. The WCET estimate must be no more than R_i, otherwise the transition can not be fired. Depth-first traversal of the reachability graph is implemented when the worst-case edge is

searched. The worst-case definition considers the usage of resources and the execution speed of the processor. Finally assembling the worst-case edge and running time of the transition fired, a special Fuzzy Petri code with additional information is generated, which is treated as source code. Source code is compiled into object source. Figure 3 is the Fuzzy Petri code of the Figure 2.

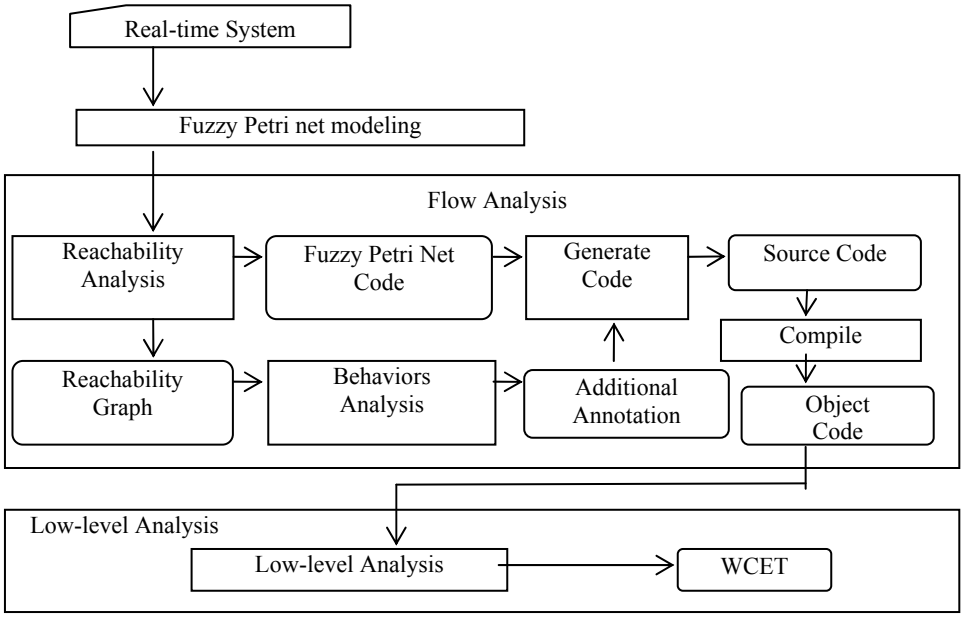


Fig.1. Architecture of WCET Estimation Analysis Based on Fuzzy Petri Net

Low-level analysis including four parts must be done. ① Each basic block of the object code is analyzed in terms of the hardware. ② The WCET of all blocks of the object code are assembled into the first WCET of the event. ③ Appropriate processor is chosen in terms of the first WCET. ④ Use the chosen processor to refine the first WCET to get the second WCET, which is the final WCET. These works must be implemented sequentially. All the program characteristics of the object code are analyzed, for example, jump and memory etc. According to the processor of which the number of processed instructions in a second is least among the processors of the system, the code characteristics are shown in form of figures to estimate the WCET of each block. Then the WCET of all blocks are assembled into the first WCET based on the relationship of program blocks and some information (such as loop number etc.). Considering the available processor task scheme, better processor is chosen. It has more free time than the processor chosen by the first WCET to run the task. The first WCET is refined by the second processor to calculate the second WCET, which is more accurate than the first one. The second WCET estimate approach decreases waste of resource and improve the processing power of the real-time system. What's more, the proposed approach refines the WCET estimate and improves the accuracy of WCET.

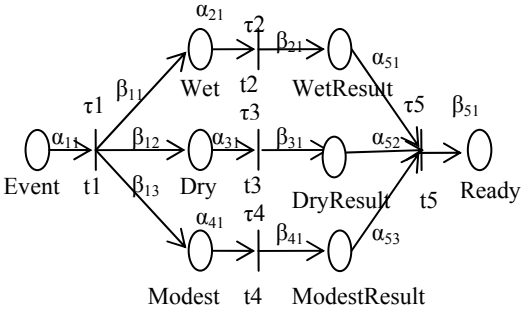


Fig.2. High-level Fuzzy Petri Net Example

```
While net is alive
If  ( f1≥ τ1)
Fire t1
If  ( f2≥ τ2)
Fire t2
If  ( f3≥ τ3)
Fire t3
If  ( f4≥ τ4)
Fire t4
If  ( f5≥ τ5)
Fire t5
End while
```

Fig.3. Fuzzy Petri Net Code

5. EMULATION ANALYSIS

To validate proposed WCET estimate method, each of datum (events) is implemented 500 and 1000 times respectively on an

operation platform, which processes a mass of datum. When the data is implemented 500 times, the longest execute time is recorded as relative WCET. The relative WCET is closer to the actual WCET, and also called fake WCET marked with W_1. When the data is processed 1000 times, the longest time is recorded as W_2. Both WECT estimation modules which are based on Matlab and Fuzzy Petri Net respectively are started up. Each data is inputted into the both WCET estimation modules to calculate the WCET respectively, which is marked with M and P. They are all recorded in the contrast table. The differences between them and W are respectively used to weigh the ability of relevant WCET estimate approaches. Table 1 shows that the values processed by the module based on Fuzzy Petri net are closer to the fake WCET than other method. Table 2 contrasts the differences based on the two estimate methods. Meanwhile the group of datum is executed 500 times and 1000 times respectively to obtain respective actual WCET estimates. Table 2 shows that the differences based on Fuzzy Petri net approach are decreased monotonically with the times increasing, namely the WCET estimate on the WCET module is closer to the actual WCET. While isolated points break decreasing trend based on Matlab method (a figure with frame in table 2), the WCET estimation is unstable. Therefore, the WCET estimate based on Fuzzy Petri net is better than other methodology.

Table 1. contrast the two WCET estimation methodologies based on Matlab and Fuzzy Petri net (n=500).

Event	Matlab(M)	Fuzzy Petri(P)	WCET(W_1)	|M-W_1|	|P- W_1|
E1	55	52	38	17	14
E2	78	72	56	22	16
E3	85	77	60	25	17
E4	117	106	87	30	19
E5	122	112	90	32	22
E6	128	120	95	33	25

Table 2. contrast the circumstances that each data is executed 500 times and 1000 times respectively.

Event	|M-W_1|(500)	|M-W_2|(1000)	|P- W_1|(500)	|P-W_2|(1000)
E1	17	15	14	12
E2	22	20	16	14
E3	25	37	17	16
E4	30	29	19	17
E5	32	30	22	20
E6	33	32	25	22

6. CONCLUSIONS

WCET estimate is an important reference to scheduling and schedulable analysis of the real-time application. It is also the basis of making sure whether periodicity tasks meet the performance and finding the bottleneck of the system ability. The paper uses the property that Fuzzy Petri net can express the concurrent tasks to model the real-time system software. The WCET estimate is executed on the high level model named Fuzzy Petri net. Contrasting the emulation results based on Matlab and Fuzzy Petri net approaches, the methodology based on Fuzzy Petri net is more valid and accurate than one based on Matlab.

REFERENCES

[1] Kligerman E, Stoyenko A. "Real-Time Euclid: A language for reliable real-time systems," *IEEE Transactions on Software Engineering*, SE-12, 1986,pp.941~949.

[2] Kirner R, Lang R, Freiberger G, Puschner P. "Fully Automatic Worst-Case Execution Time Analysis for Matlab/Simulink Models" [A]. *EUROMICRO Conference on Real-Time Systems*, 2002,pp.31-40.

[3] Erpenbach E, Stappert F, Stroop J. "Compilation and Timing Analysis of Statecharts Models for Embedded Systems" [A]. *The Second International Workshop on Compiler and Architecture Support for Embedded Systems (CASES'99)*, Washington, D.C, Oct. 1999.

[4] Erpenbach E. Compilation, "Worst-Case Execution Times and Schedulability Analysis of Statecharts Models," PhD thesis, University of Paderborn, Germany, 2000.

[5] Healy C.A, Arnold R.D, Mueller F. "Bounding Pipeline and instruction cache performance" [J]. *IEEE Transaction on Computers*, 1999,pp.53~70.

[6] Stappert F, Altenbernd P. "Complete worst-case execution time analysis of straight-line hard real-time programs" [J]. *Journal of Systems Architecture*, 2000 ,pp.339-355.

[7] Puschner P, Koza C. "Calculating the maximum execution time of real-time programs," *Real-time systems*, 1, 1989,pp.159~176.

[8] Shaw A.C. "Reasoning about time in higher-level language software," *IEEE transactions on software engineering*, SE-15,1989,pp.875~889.

[9] Li Y.S, Malik S. "Performance analysis of embedded software using implicit path enumeration" [A]. *Proc. of the ACM SIGPLAN workshop on language*, compilers and tools for real-time system, 1995.,pp.95~105.

[10] Li Y.S, Malik S, Wolfe A. "Efficient micro-architecture modeling and path analysis for real-time software" [A]. *Proc. 16th IEEE real-time system symposium*, 1995,pp.298~307.

[11] Li Y.S, Malik S, Wolfe A. "Cache modeling for real-time software: beyond direct mapped instruction caches" [A]. *Proc. 17th IEEE real-time system symposium* ,1996.

[12] Engblom J, Ermedahl A. "Modeling Complex Flows for Worst-Case Execution Time Analysis" [A]. *Proc. 21st IEEE Real-Time Systems Symposium (RTSS'00)*, Nov. 2000,pp.163-174.

[13] Gustafsson J. "Analyzing Execution-Time of Object-Oriented Programs Using Abstract Interpretation" [D]. PhD thesis, Department of Computer Systems, Information Technology, Uppsala University, May 2000.

A Routing Protocol with Link Status Predicting in Mobile Ad hoc Network *

Jin Lian[1,2], Layuan Li[1], Xiaoyan Zhu[2], Baolin Sun[3]
[1]School of Computer Science and Technology, Wuhan University of Technology
Wuhan, 430063, P.R.China
[2]School of Mathematics & Computer Science, JiangHan University
Wuhan, 430056, P.R.China
[3]College of Computer & Technology, Hubei University of Economics
Wuhan, 430205, P. R. China
Email: lj_jhun@163.com

ABSTRACT

In Mobile Ad Hoc Network (MANET) due to the dynamic nature of the network topology and restricted resources, the real traffic and stability of every link is commonly not same. This paper presents a stability Routing Protocol with Link Status Predicting in MANET (LSPRP). The key idea of LSPRP algorithm is to use GPS to forecast the link Stability and estimate the nodes traffic so as to provide stability guarantee in the ad hoc network. The simulation results shows that the LSPRP approach provide an accurate and efficient method of estimating and evaluating the route stability in dynamic mobile networks.

Keywords: Motion Predicting, MANET, Routing Protocol, Link Status, AODV.

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. There is no static infrastructure such as base station as that was in cell mobile communication. All the nodes are free to move around randomly, thus changing the network topology dynamically. For such networks, an effective routing algorithm is critical for adapting to node mobility as well as possible channel error to provide a feasible path for data transmission [1-7].

Link Status Predicting can discover a Stability routing and avoid low quality paths. The basic idea is firstly to find some Stability routing paths, and then according to the realistic traffic of node maintain routing paths. Therefore, we can guarantee performance with realistic accuracy.

In this paper, we present a Stability Routing with Link Status Predicting in Mobile Ad hoc Network (LSPRP).

The rest of the paper is organized as follows: Section 2, depicts the link status predicting mechanism. Section 3, presents a stability routing protocol with link status predicting. Section 4, provides simulation results. Section 5, describes the conclusion.

2. LINK STATUS PREDICTING MECHANISM

In this paper, we adopt Link Status Predicting Mechanism including two aspects----Motion Predicting Mechanism and Nodes Traffic Estimating Mechanism. Motion Predicting Mechanism guarantees the link's usability and reliability. Nodes Traffic Predicting Mechanism guarantees the efficiency of the data transmission in the links.

In Motion Predicting Mechanism, we assume a free space propagation model [6], where the received signal strength solely depends on its distance to the transmitter. We also assume that all nodes in the network have their clock synchronized; If the motion parameters of two neighbors (such as speed, direction, and radio propagation range) are known, we can determine the duration of time these two nodes will remain connected. Assume two nodes i and j are within the transmission range ra of each other. Let (xi, yi) be the coordinate of mobile host i and (xj, yj) be that of mobile host j. Also let vi and vj be the speeds, and θi and θj ($0<=\theta i, \theta j < 2\pi$) be the moving directions of nodes i and j , respectively. Then, the amount of time two mobile hosts will stay connected, LET, is predicted by [6]:

$$LET = \frac{(ab + cd) \pm \sqrt{(a^2 + c^2) r_a^{\,2} - (ad - bc)^2}}{a^2 + c^2}$$

where

$$a = v_i \cos\theta_i - v_j \cos\theta_j$$
$$b = x_i - x_j$$
$$c = vi \sin\theta_i - vj \sin\theta_j$$
$$d = y_i - y_j$$

Note that when vi = vj and θi =θj, t becomes ∞. The predicted value is the link expiration time (LET) between the two nodes. If the LET is long, the load on the network increases because of the frequent route request. In the opposite case, it is difficult to implement the mobile predicting. On the assumption that τ is the average transfer delay and if LET > τ ,the link is stable. Otherwise the link is not stable. Using the Motion Predicting Mechanism, we can obtain a stably and reliably link in Mobile Ad Hoc Networks.

In MANET, the traffic of every node is different. The real traffic of a node is commonly concentrated in a small number of particular nodes [4]. This characteristic has not been considered in the design of the existing routing algorithms. Therefore, it is difficult to guarantee the efficiency of data transfer. The Nodes Traffic Estimating Mechanism is that the additional RREQ messages are frequently sent in order to access nodes. There are two additional fields in each destination entry in the routing table: the Counter and the Select-RREQ. Each node examines the packet type when transmitting the packet. If it is the data packet, the Counter value for the destination increases. If it is the control packet, the Counter value is not changed. According to the Counter value, we can easily get hold of the number of packets transmitted to a destination. Let RREQ-Entry-Selection-Time and Select- RREQ-Time be the periods to select the frequently accessed nodes and to send the additional RREQ messages, respectively [4]. Thereby, we send the additional RREQ

* This work is supported by a grant from National Natural Science Foundation of China (No.60672137), the Ph.D. Programs Foundation of Ministry of Education of China (No.20060497015), NSF of Hubei Province of China (No.2006ABA301).

messages for frequently accessed nodes to continuously maintain the routing paths in the routing table. By doing so, the packet is sent faster and the data communication is more stable for a network topology that changes rapidly.

3. LINK STATUS PREDICTING ROUTING PROTOCOL (LSPRP)

LSPRP is based on the AODV routing protocol and make use of Link Status Predicting Mechanism. First, we extend the RREQ and RREP package in the AODV.A field that denote the link stabilization (namely LET) is added in the RREQ package, and the RREQ package also includes the position, speed, moving direction of the mobile host. For the RREP package, we add a field that denotes the identifier of the link stabilization .If the field value is one, the link is stable, otherwise the link is not stable.

The Route Discovery of LSPRP Algorithm is designed as follows:
Step1: If the route to destination host exists, the package is direct sent. Otherwise, using the RREQ package broadcast the destination host and the LET is set to the maximum.
Step2: According to the motion predicting mechanism, the host that receives the RREQ computes the LET between itself and upriver-host. If the current value is more, the LET equals the current value.
Step3:The destination host receives the RREQ, computes the LET of upriver-host and deal with according to step2.Then the host waits for other RREQ in τ .
Step4: The destination host computes LET in other RREQs, obtains the maximum of LET and sends the RREP package. If LET > τ ,the field that denotes the identifier of the link stabilization is set one. Otherwise the value of the field is zero.
Step5: When the host receives the RREP, the host adds the value of the identifier of the link stabilization to routing table.
Step6: Each host searches the Counter values in its routing table entries and determines the RREQ-Entry-Number nodes with the largest values. The Select- RREQ values of these nodes are set to one. Each node sends additional RREQ messages to the destination nodes every Select- RREQ- Time if the Select RREQs corresponding to those nodes equals one. Then, the Counter values in the routing entries are initialized to zero in order to rapidly adapt to the changes in the network. These procedures are consecutively repeated every RREQ-Entry-Selection-Time.

The route maintenance of LSPRP algorithm includes: when the value of the identifier of the link stabilization is one in the routing table, the host computes the value of t using predicting model compute. If LET > τ ,the link is stable. Otherwise the source host sends routing request over again. When the value of the identifier of the link stabilization is zero in the routing table, the host adopts the passiveness maintenance with AODV.

4. SIMULATION

We simulated the proposed scheme in ns2 [8] and conducted experiments to evaluate the effectiveness of the proposed scheme. The network environment for the ns2 simulator is given in Table 1. To evaluate the LSPRP, it is compared with the AODV routing protocols. In this performance evaluation the following performance metrics were evaluated: percentile of data transmission rate, path success ratio, and average packet delay.

Fig.1 depicts a comparison of data transmission rate AODV and LSPRP scheme. The data transmission rate is still higher than that of AODV, which means it is more suitable for the routing choosing under timely data transmission application and dynamic network structure. The average packet delay performance as shown in the Fig.2 proves that the packet delay improves when scheme is included.

Table 1. Simulation Setting

MAC Layer	IEEE802.11
Simulation Area	1000 x 1000
Simulation Time	300
Mobile Nodes	30
Node Mobility Speed	0-10m/s
Node Moving Pattern	Random Way Point
Traffic Type	CBR
Packet Size	512byte
Number of Connection	50
Active Route Timeout(AODV)	10s
The average end to end delay τ	0.2
transmission range	250
RREQ-Entry-Number	5
RREQ-Entry-Selection-Time	3
Select-RREQ Time	10s
the realistic traffic of node	35% 80% 95%

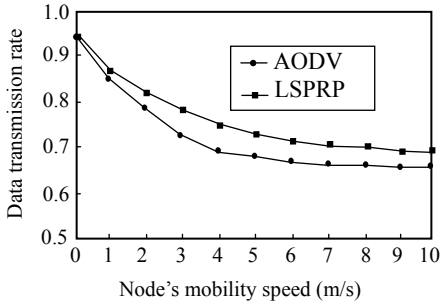


Fig.1. Data transmission rate vs. Node's mobility speed

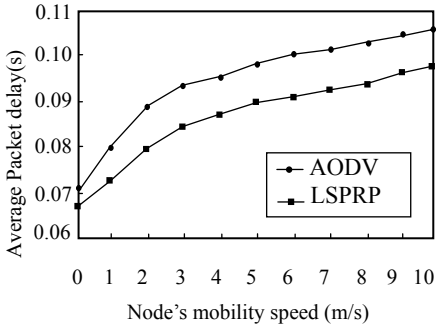


Fig.2. Average packet delay vs. Node's mobility speed

5. CONCLUSIONS

In this paper, we present a stability routing with Link Status Predicting in MANET (LSPRP). LSPRP adopts Motion Predicting Mechanism and Nodes Traffic Estimating Mechanism in order to establish the stable links, provides a quick response to changes in the network and minimizes the waste of network resources. LSPRP algorithm has produced

significant improvements in data transmission rate, and average end-to-end delay.

REFERENCES

[1] Sun, B. L., and Li, L. Y, "A QoS Multicast Routing Optimization Algorithms Based on Genetic Algorithm," *Journal of Communications and Networks*, Vol. 8, No.1, 2006，pp.116-122.

[2] Sun, B. L., Li, L. Y., Yang, Q., and Xiang, Y, "An Entropy-Based Stability QoS Multicast Routing Protocol in Ad Hoc Network," *Advances in Grid and Pervasive Computing (GPC 2006),* Lecture Notes in Computer Science, Vol. 3947, Springer-Verlag Berlin Heidelberg, 2006, pp.217-226.

[3] Sun, B. L., Yang, Q., Ma J. and Chen H, "Fuzzy QoS Controllers in Diff-Serv Scheduler using Genetic Algorithms," *Computational Intelligence and Security (CIS2005)*, Lecture Notes in Artificial Intelligence, Vol. 3801, Springer-Verlag Berlin Heidelberg, 2005,pp. 101-106.

[4] Tae-Eun Kim, Won-Tae Kim, and Yong-Jin Park, "Selective Route Discovery Routing Algorithm for Mobile Ad-Hoc Networks," *The International Conference on Information Networking(ICOIN2005)*, Lecture Notes in Computer Science, Vol. 3391, Springer-Verlag Berlin Heidelberg, 2005, pp.152-159.

[5] Perkins, C., Royer, E. B., and Das, S.: Ad hoc On Demand Distance Vector (AODV) Routing. RFC 3561, Jul 2003.

[6] William Su, Sung-Ju Lee, and Mario Gerla, "Mobility Prediction in Wireless Networks," *21st Century Military Communications Conference Proceedings(MILCOM 2000)*, Los Angeles, CA, USA,Volume1, Oct 2000, pp.491-495.

[7] Sun, Q., Li, L. Y, "An Efficient Distributed Broadcasting Algorithm for Ad Hoc Networks," *Advanced Parallel Processing Technologies (APPT 2005)*, Lecture Notes in Computer Science, Vol. 3756, Springer Verlag Berlin Heidelberg, 2005, pp.363-372.

[8] "The NS Manual, A Collaboration between researchers at UC Berkeley, LBL, USC/ISI and Xerox PARC," Available at http://www.isi.edu/nsnam/ns.

Jin Lian is a PhD student of Computer Science and Technology, Wuhan University of Technology. He graduated from Hubei University in 1998; from University of Science and Technology of China in 2004 with specialty of software engineering. He is a prelector of Mathematics & Computer Science, JiangHan University. His research interests are in mobile ad hoc network routing protocol, software testing and software development method.

Design and Implementation of the Mobile Navigation and Positioning System Based on PDA

Bo Chen [1,2], Zexun Geng [2], Yang Yang[1], Maolin Wang [1], Jing Yang [1]
[1] Guilin Air Force Academy, Guilin, Guangxi 541003, China
[2] Institute of Surveying and Mapping, Information Engineering University, Zhengzhou, Henan 450052, China
Email: [1]hb43chenbo@163.com

ABSTRACT

The mobile navigation and positioning system is used to carry out dynamic auto-navigation of mobile objects. The key technologies, such as spatial vector data storage and management, spatial topology generation, spatial index generation, receiving and computation of positioning data, map matching etc, are emphatically analyzed. At last, the paper presents the implementation and application of the mobile navigation and positioning system based on PDA.

Keywords: Mobile Navigation Positioning System, PDA, Windows CE, GIS

1. INTRODUCTION

Thanks to the development of technology on computer software and hardware, the successful application of WAP wireless internet technology and the appearance of all kinds of mobile intellective terminal with the function of wireless internet technology (such as PDA, WAP cell phone etc), people can accomplish all work which were only done at office or home before, namely, 'mobile working'. Intellective terminal plus wireless internet have already been applied to all aspects of life successfully. Meanwhile, the appearance of peripheral hardware (such as GPS, GSM, etc.), which suit to these intellective terminals, further expands the terminals' application domain. Went without saying, the application of these new technologies, such as intellective terminals, GPS, wireless internet etc, will certainly enrich the theory and expand the domain of GIS. The integration of GIS and GPS plus wireless internet based on these intellective terminals platform will inevitably become a rising important research domain of GIS. The integrative research on GIS and GPS plus wireless internet is called 'Mobile GIS' [1-2] by International GIS group.

The mobile navigation and positioning system is a mobile GIS system which is based on the hardware platform of PDA and developed on the operating system Windows CE. Based on the conventional GIS, the system is essentially a spatial information application system with digital maps in the background, which can realize real-time positioning by utilizing space orientation of satellite positioning system and embedded technology. The mobile navigation and positioning system can be applied to many domains such as military and national defense, intellective car, intellective traffic, informative consumer equipment, industrial control, environmental engineering and so on[3]. This paper aims at the design and development mobile navigation and positioning system on the platform of Windows CE and gives some preliminary discussion.

2. SOME KEY TECHNOLOGIES

2.1 Storage and Management of Spatial Vector Data

Data is the foundation of GIS, whether the data format is defined well or not will directly influence the effect and speed of each functional module, and even determine whether some certain function can realize or not. The data format of mobile navigation and positioning system is so much more, and it determines the storage size of vector data and directly influences the performance of map display and spatial query [4-5].

The mobile navigation system designs a GIS data format that is derived from national map digitalization standard and operated on PDA. It includes various basic data elements whose organizing and distributing mode is convenient in the program design. It can load source data of diverse form and compresses vector data to a great ratio by the format conversion.

In the system we adopt the data type that has less capacity and delete unnecessary data to make vector data concise and perfect. By saving all the data in binary system, it can not only be more secure but reduce the capacity of data. The experiment proves that the compression ratio of data of a normal topographic map of 1 ratio 50000 can reach 10 times ratio or so when processed. Taking a breadth of vector data of 8 MB for example, the data become 400 KB-800 KB. Now the popular 32-MB-memorizer of PDA can store about 20 maps like this except the capacity occupied by operation system and application software, this solves storage capacity of vector data basically. For the further use, the data can be stored in exterior expanded memory cards (such as CF card, SD card, etc.). At present, these cards have reached the max storage of 1G, which can completely satisfy the need of mobile users. If you carry out the real-time transmission of vector data on the condition of perfect communication system, it can solve the problems of data storage and updating much better.

2.3 Spatial Topology Generation [6-7]

This system needs to match positioning data and spatial vector data, but lots of vector map data run short of complete spatial topological relation, it is necessary to reconstruct the spatial topology relation for vector map data. The auto topology algorithms' basic steps and key points include: chain organizing, crunodes matching, checking polygon close or not, constituting polygon, judging island, confirming property of polygon.

The system designs an effective spatial relationship data format which adopts the idea of object-oriented modeling and partial model on the basis of comparing existing spatial data model. It automatically generates spatial topology relation and interior point by grid index broken chain of line group self-intersection and intersection and Minimum Bounding Rectangle. The generation of auto topology relation is:

1) Breaking chain: arch section breaks automatically, which makes the picture have no self-intersection and intersection arch section;
2) Crunodes matching: network topology relation between points and arch section is constituted;

3) Constituting polygon: track left handed rotation arithmetic and right handed rotation arithmetic, then create polygon and constitute the relation between polygon and arch section;
4) Interior point generating: generate interior point of polygon automatically;
5) Nesting relation generating: constitute polygon nesting relation tree, find out 'island' included in polygon and constitute relations between polygons;
6) Surface number adjustment: adjust the number of left and right surface for relating arch section of nest relation polygon.

2.3 Spatial Index Generation

In order to improve the performance of graphical display and spatial query, spatial index technology must be adopted. Spatial index refers to the data structure arranged according to motive sequence based on position, shape and certain spatial relation of spatial object. It is crucial to raise storage efficiency of spatial data. Typical spatial index is commonly of spatial data structure that's top-down and space partitioned gradually. The representative spatial indexes are BSP, K-D-B tree, CELL tree and grid index etc.

To generate spatial index on PDA, it needs to consider both internal memory of PDA and processing capacity of microprocessor, which is for reducing the algorithm's complexity and shortening search time. After comparing present spatial index technology, according to the idea of grid index, the spatial index method based on minimum circum rectangle is adopted. That is, by computing vertex coordinates of linear and area feature, the minimum circum rectangle of each not-point element is obtained and stored into RAM. When indexing, the minimum circum rectangle of each not-point element are compared, if it is inside the rectangle or intersects with the rectangle, then it is computed to see whether it is index object, otherwise, the next element is searched until index object is found. The arithmetic is easy, effective and less occupied space, its search rate can advance 2-3 times.

2.4 Receiving and Computation of Positioning Data

To exploit GPS data computation software on PDA, the first problem to be solved is serial-port communication between PDA and GPS receiver. During the communication between PDA and GPS receiver, as the code converter between CPU and serial device, the PDA's serial port provides the data transmission channel between GPS and PDA. As data terminal device, GPS receiver adopts asynchronous serial mode that utilizes RS-232 serial binary data to exchange cable interface and then transmit collective data to PDA by the serial port. PDA can read GPS positioning data according to the corresponding format (such as NMEA0183 protocol), and then transform positioning data from WGS-84 to GAUSS-80 coordinate system, and finally realizes mobile object point's positioning by map matching [8]. The data flow refers to Figure 1.

Because GIS software employs CPU much more, meanwhile, convenient timer controlling communication occupies CPU much and it can't deal with data real-timely, which will reduce the whole system's efficiency and even lose data. This system adopts multithread to realize the communication between GPS receiver and PDA, and make full use of Windows CE's multi-task and multi-thread to use CPU efficiently and make the whole system much more efficient and stable.

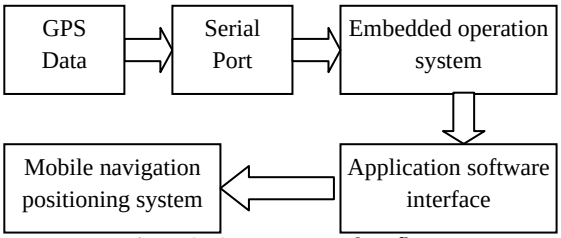


Fig.1. GPS positioning data flow

2.5 Map Matching

Map matching is a method that matches GPS positioning data with road level data in GIS to eliminate or reduce the effect brought by all sorts of error and makes object's positioning accurate on road level. It assumes that car runs on road all along. Present map matching methods include line shortest distance, probability statistics, and network topology relation and so on. The precondition of later two is that it must have the support of correct history matching result, and current position of car will be matched on the basis of the results. In the analysis of the course of map matching in positioning and navigation system, all the possible cases in map matching mainly include these two aspects: GPS data receiving status and road topographic feature. There are three kinds of GPS data receiving status: valid data normally received bigger drift error and no signal. Road topographic feature which effects map matching also include three cases: collateral road, conjunction and bifurcate point.

In this system, we design an algorithm that matches map by history track deducing. The history track deducing method constitutes a car dynamic model in terms of car running status and road surroundings, and then gets the current position of car according to the running history track. The positioning precision of the method depends on the quality of the constructed car dynamic model, meanwhile, it is carried out when GPS data is invalid, car normally runs and doesn't have long time stop and only car running doesn't overstep the topology section of a highway. When GPS has exterior abrupt error such as no signal or bigger drift error the method can match intellectively and realize car real-time dynamic navigation.

3. MOBILE NAVIGATION AND POSITIONING SYSTEM BASED ON PDA

Mobile navigation and positioning system essentially is a system that provides with real-time positioning of mobile object, surroundings information and various of instruction information on the basis of conventional GIS, utilizing a certain spatial positioning measure such as GPS, inertial navigation and so on and on the display background of digital map. Mobile objects mainly refer to ambulatory or well-traveling-performance objects such as person, ship, car and so on. Under the circumstance of comprehensive consideration all kinds of requirement for customer use and relevant level of software and hardware, mobile navigation and positioning system is designed on the platform of PDA, synthesizing satellite navigation and positioning, embedded technology, GIS technology and so on. This system is composed of 9 modules which is positioning, communication, GIS engine, path analysis, path steering, map matching, electronic map database for navigation, map database and human-computer interaction interface. The architecture refers to Fig. 2.

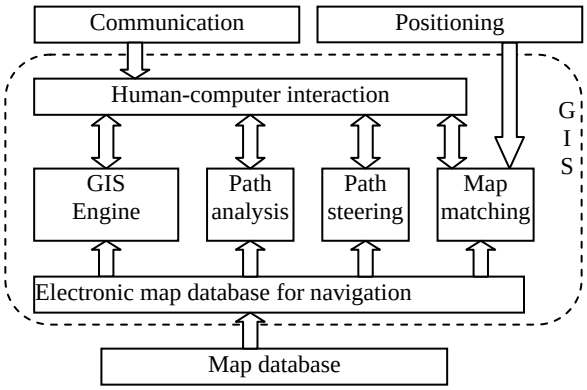


Fig.2. The architecture of mobile navigation and positioning system

This system uses the PDA of LEGEND TIAN JI XP210 as the mobile terminal. The GPS receiver is Compact GPS which is connected with CF card of PDA and has interior and exterior antennae, 12 channels and supporting NMEA0183 protocol. The source data format transmission section is performed with the platform of Visual C++ 6.0 on normal PC. The operation system of PDA is Windows CE 3.0 (Pocket PC 2002), and the developing platform is Microsoft Embedded Visual C++ 3.0 and Microsoft Visual C++ 6.0. One interface for this system running on the emulator refers to figure 3 and figure 4. The experimental data in the figures is in Zhen Zhou, China.

Fig.3. The map level management interface of the Mobile Navigation and Positioning System.

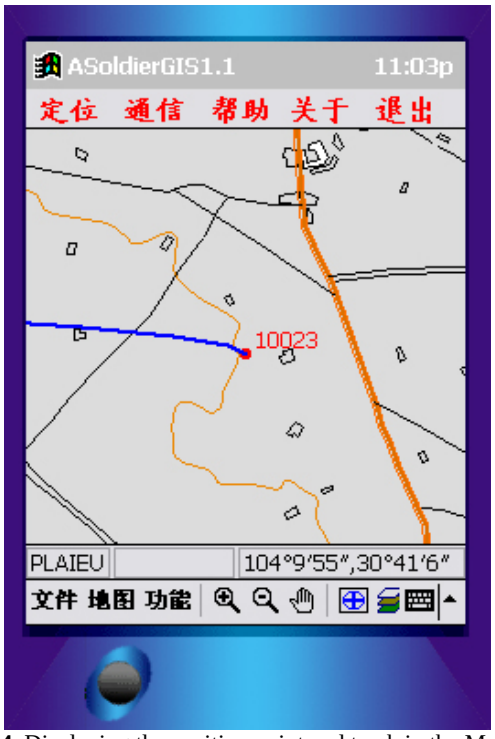


Fig.4. Displaying the position point and track in the Mobile Navigation and Positioning System.

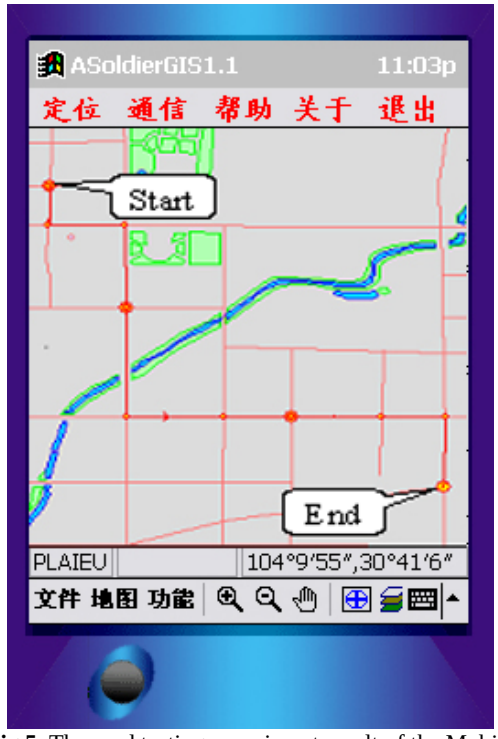


Fig.5. The road testing experiment result of the Mobile Navigation and Positioning System

4. CONCLUSIONS

As a independent system, mobile navigation and positioning system can satisfy with user's requirement for acquiring current geographic position information and in most cases it is a essential user terminal section in many integrated mobile monitoring and controlling systems. It can satisfy with the requirement for geo information acquisition, mobile object

distribution and information interaction such as public security, fire protection, traffic, tour, medical treatment, insurance, post expressage, field measurement, proving, gathering and saving, military affairs and so on. This system is united closely with trade trait so it has extensive application foreground.

REFERENCES

[1] Zhang S H, and Fang Yu, "The Significance and State of The Art of Mini-type Embedded GIS Software Platform," *China. J. Image&Graphics*, Vol.9, 2001, pp.900~906.

[2] Zhang Qiang, Wang Renli, and Chen Tianze, "Embedded GIS Developing and Application Based on Windows CE Platform," *Journal of Zhengzhou Institute of Surveying and Mapping*, Vol.20, No.2, 2003, pp.113~116.

[3] Zhao Yilin, *Car Positioning and Navigation System*, Publishing House of Electronic Industry, Beijing, China ,1999.

[4] Hua Yixin, Wu Sheng, and Zhao Junxi, *The Theory and Technology on Geographical Information System*, PLA Press, Beijing, China, 2001.

[5] Chen Bo, *The Research on Monitoring and Controlling Battlefield Situation Based on Satellite Navigation System*, Zhengzhou Information Engineering University, Zhengzhou, China, 2005.

[6] Zhan F B, "Three Fastest Shortest Path Algorithms on Real Road Networks," *Journal of Geographic Information and Decision Analysis*，Vol.16, No.1, 1997, pp.69～82.

[7] Huang Y H, Rundensteiner E A and Jing N, "Evaluation of Hierarchical Path Finding Technologies for ITS Route Guidance," *In Proceedings of 1996 Annual Meeting of ITS*, American, 1996, pp.340～350.

[8] G.Derekenaris, J.Garofalakis and C.Makris, "Integrating GIS ,GPS and GSM technologies for the effective management of ambulances," *Computers, Environment and Urban Systems*, No.25, 2001, pp.267～278.

Bo Chen was born in 1981. He received the B. Eng. degree in science & technology of remote sensing and M.Eng. degree in photogrammetry and remote sensing from Information Engineering University, Zhengzhou, China, in 2002 and 2005. He is currently pursuing the Ph.D. degree at Institute of Surveying and Mapping, Information Engineering University of PLA. He has published one book, over 30 papers. His research interests include mobile GIS and image super-resolution.

Measurement for Phase and Period Oscillation of TCP Dynamic

Wei Zhou[1], Bing Zhu[2], Xiangjun Wang[3]
[1]Department of Computer Sciences and Technology,
HuaZhong Normal University, Wuhan, 430079, P.R.China
[2]Futian Foreign Language School,
Seven Street Jintian Bei Futian District, Shenzhen, Guangdong ,518034,P.R.China
[3]Department of Computer Sciences and Technology,
HuaZhong Normal University, Wuhan, 430079, P.R.China
E-mail: [1]zhouwei_2600@hotmail.com, [2]zhubing831007@163.com,[3] wangxiangjun@mails.ccnu.edu.cn

ABSTRACT

This paper is aimed to describe a technique for estimation of local signal frequency and bandwidth. In this paper we propose a formula to measure the period oscillation of TCP dynamic. We use different approaches that allow us to describe the phase and frequency in a reasonable way. Furthermore, we present the Fourier series as a new method to denote the window update. We define the transmission rate as an analytic signal, in this situation we can obtain the instantaneous phase easily and compared with our experiment result. From this paper you can know that some parameters can be changed in order to avoid the transmission synchronous, and improve the utilization of the bandwidth.

Keywords: Instantaneous Phase, Analytic Signal, Period Oscillation

1. INTRODUCTION

This paper describes a technique for estimation of local signal frequency and bandwidth. Local frequency is an important concept useful for local structure analysis as well as for determining the appropriate range of scales for subsequent processing. Our method is based on combining local estimates of instantaneous frequency over a large number of scales. The bandwidth is used to produce a measure of certainty for the estimated frequency [7]. The theory of phase synchronization is so mature. For any signal $s(t)$, there are so many methods to obtain the instantaneous phase. When talking about the oscillation, there are two statuses. First, it's the period oscillation. You can read [1] to learn more. Second, it is the phase of a chaotic oscillator. It seems to be no unambiguous and general definition of phase applicable to an arbitrary chaotic process. Reference [2] refer that: the instantaneous phase of any signal $\{ x(t) \}$ is:

$$\phi(t) = \tan^{-1} \frac{x_H(t)}{x(t)} \qquad (1)$$

where $\{ x_H(t) \}$ is the Hilbert transform of $\{ x(t) \}$, and the general condition for phase synchronization between two coupled non-linear oscillators is defined as: $\varphi_{n,m} = | n\phi_1(t) - m\phi_2(t) | < \alpha$,where n and m are positive integers, $\phi_{1,2}$ are the phases of two oscillators , and α is an arbitrary constant.

A signal that has no negative-frequency components is called an analytic signal. If we want to measure the period oscillation of the transmission rate, we have to determine the amplitude and the phase of the rate $x(t)$. For periodic oscillations, in Reference [1] the authors remind that stable periodic self-sustained oscillations are represented by a stable limit cycle in the phase space, and the dynamics of a phase point on this cycle can be described as:

$$\frac{d\phi}{dt} = \omega_0 , \qquad (2)$$

where $\omega_0 = 2\pi / T_0$, and T_0 is the period of the oscillation. From Reference [3], we can also see that the mean frequency defined as the average of $d\phi_p / dt$ over a large period of time, where ϕ_p is the instantaneous phase.

In contrast to the dynamics of the phase of periodic oscillations, the growth of the phase in the chaotic case cannot generally be expected to be uniform. Instead, the instantaneous frequency depends in general on the amplitude, so we can write as in Reference [4]

$$\frac{d\phi}{dt} = \omega + F(A) \qquad (3)$$

The term $F(A)$ describes the dependence of the instantaneous frequency on the amplitude $A(t)$, which we assume to be chaotic.

2. OUR MODEL AND EQUILIBRIUM

In this paper, we consider the network transmission rate $x(t)$ as an analytic signal. For an arbitrary signal $s(t)$, we can determine the amplitude and the phase [5]. The analytic signal $\psi(t)$ is a complex function of time defined as

$$\psi(t) = x(t) + jx_H(t) = A(t)e^{j\phi(t)} \qquad (4)$$

Where the function $x_H(t)$ is the Hilbert transform $x(t)$

$$x_H(t) = \pi^{-1} P.V. \int_{-\infty}^{\infty} \frac{x(\tau)}{t-\tau} d\tau \qquad (5)$$

(Where P.V. means that the integral is taken in the sense of the Cauchy principal value). $A(t)$ is the instantaneous amplitude and $\phi(t)$ is the instantaneous phase. So we can obtain

$$x(t) + jx_H(t) = A(t)(\cos\phi(t) + j\sin\phi(t)) \qquad (6)$$

from the equation (6), we can gain

$$\phi(t) = \arctan \frac{x_H(t)}{x(t)} \qquad (7)$$

This is the instantaneous phase of the transmission rate $x(t)$. At the same time, over a large period of time the mean frequency ω of the rate can be defined as:

$$\omega = \frac{d\phi}{dt} = (\arctan \frac{x_H(t)}{x(t)})' = \frac{x(t)x_H'(t) - x'(t)x_H(t)}{x_H^2(t) + x^2(t)} \qquad (8)$$

From (8), we can get the instantaneous frequency. The notion of instantaneous frequency is used for narrowband analysis over a number of scales. The estimates are weighted and summed to produce a wide band frequency estimate.

So the mean period T= $\frac{1}{\omega}$, then

$$T=\frac{x_H^2(t)+x^2(t)}{x(t)x_H^{'}(t)-x^{'}(t)x_H(t)} \quad (9)$$

If we suppose the RTT (round-trip time) is a constant. The transmission rate can be defined as:

$$x(t)=\frac{w(t)}{RTT} \quad (10)$$

where the $w(t)$ is the window update. From (9), we can obtain:

$$T=\frac{w_H^2(t)+w^2(t)}{w(t)w_H^{'}(t)-w^{'}(t)w_H(t)} \quad (11)$$

where the $w_H(t)$ is the Hilbert transform of $w(t)$.

The above that we obtained is local information. It is noteworthy that, despite their names, instantaneous phase and instantaneous frequency are global entities. The local behavior is since long recognized as important property for signal processing [7].

Modern implementations of TCP contain four intertwined algorithms: slow start, congestion avoidance, fast retransmit, and fast recovery. For different algorithms of TCP, the window update may be measure in different ways. In this paper we talk about the slow-start [6]. In slow start, when a connection is established, the value of cwnd is first set to 1 and after each received ACK the value is updated to
cwnd = cwnd + 1

implying doubling of cwnd for each RTT. The exponential growth of cwnd continues until a packet loss is observed, causing the value of ssthresh to be updated to
ssthresh = cwnd/2.

After the packet loss, the connection starts from slow start again with cwnd = 1, and the window is increased exponentially until it equals ssthreshp [7] [8].

When the transmissions begin, the window size gradually reaches a peak W. When a packet is dropped, the congestion window is halved. After the drop, the TCP sender increases linearly its congestion window until the congestion window has reached its old value W and then another packet drop occurs. The development of TCP's congestion window under these assumptions is depicted in Fig.1.

So we can suppose the window update $w(t)$ is a period function, and the mean period is $L=2l$. The function $w(t)$ is integrabel in the area $(0,2l)$. So we propose a new method to measure the window update using the Fourier series.

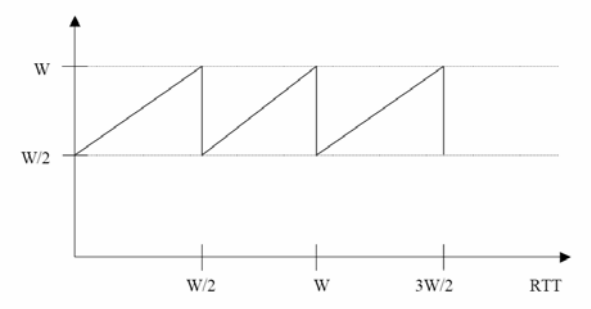


Fig.1. Development of TCP's congestion window

$$w(t)\cong\frac{1}{2}a_0+\sum_{n=1}^{\infty}(a_n\cos\frac{n\pi}{l}t+b_n\sin\frac{n\pi}{l}t) \quad (12)$$

where a_n, b_n are the Fourier coefficient,

$$a_n=\frac{1}{l}\int_0^{2l}w(t)\cos\frac{n\pi}{l}tdt \quad (n=0,1,2\cdots\cdots) \quad (13)$$

$$b_n=\frac{1}{l}\int_0^{2l}w(t)\sin\frac{n\pi}{l}tdt \quad (n=1,2,3\cdots\cdots) \quad (14)$$

For the packet loss process is a Poisson process, that is, in the time $(0,t)$ the packet loss number $N(t)$ subject to the Poisson distributing. So the period L of $w(t)$ subject to the exponential distributing. The distribution function of L can be defined as:

$$F(t)=P(L<t)=1-e^{-\lambda t},\ (t>0) \quad (15)$$

Where the λ can be considered as the packet loss rate.

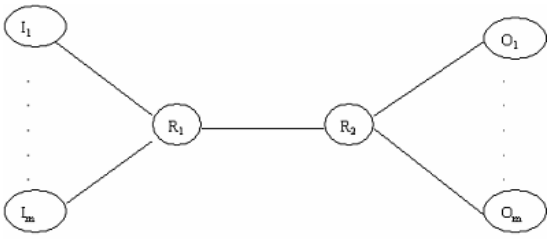


Fig.2. Control model

In this paper, we consider the control model like Fig.2. We suppose there are m input nodes and m output nodes; they all pass one road from R_1 to R_2. By combining the outputs from two or more sets of nodes that differ only in center frequency ω_n, it is possible to produce a local frequency estimate. In fact, in the network, when the transmission rate is synchronous, the rush may be appearance. From our estimate, we can change the congestion window to avoid the synchronous, and use the bandwidth efficient.

3. SIMULATIONS AND RESULT

To test the new method of measurement, we used NS2 and Matlab.

In the simulations we set the nodes number $m=3$. Using some signal process method, we know that the broader the bandwidth, the weaker the notion of instantaneous frequency

becomes [9]. So we choose the bandwidth of every links 10Mbps. The three sources share one public link; they send the packet at the same time.

The following figures (Fig.3, 4, 5) show the measurement of the window update of three sources under Reno, Vegas, Fast. The figures (Fig.6, 7, 8) show the estimate of the instantaneous phase of three sources under different TCP protocol. From these figures we can see that the window update is basically synchronous. And the instantaneous phase is also basically synchronous. We can also see that different TCP protocol the synchronous period is different.

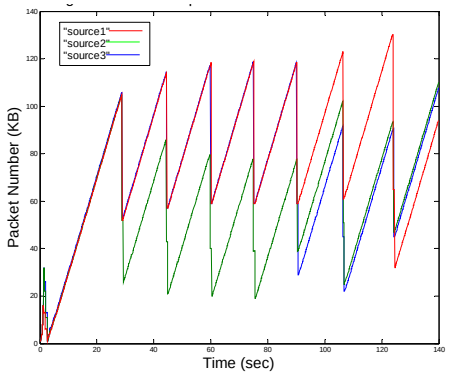


Fig.3. The window update of three sources under Reno

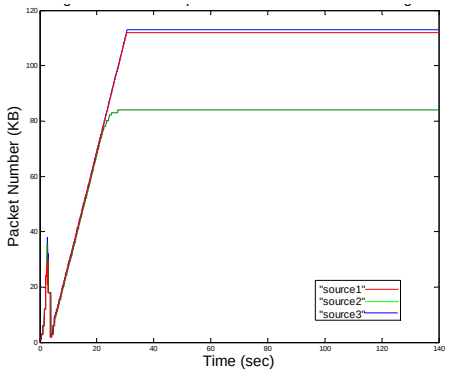


Fig.4. The window update of sources under Vegas

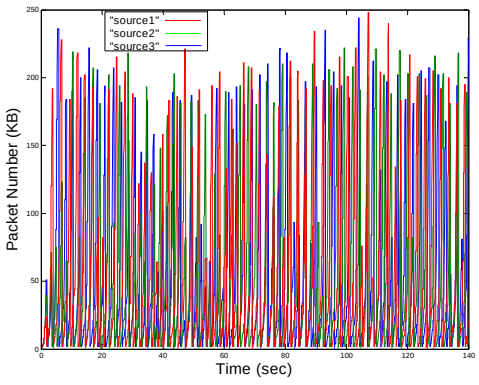


Fig.5. The window update of three sources under Fast

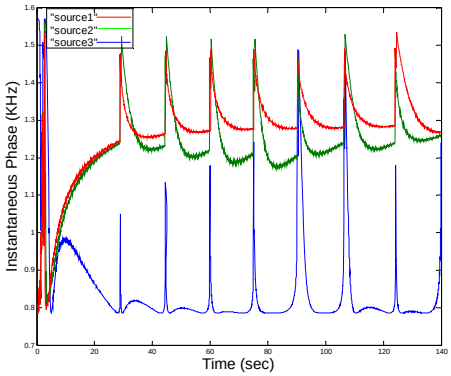


Fig.6. The instantaneous phase of three sources under Reno

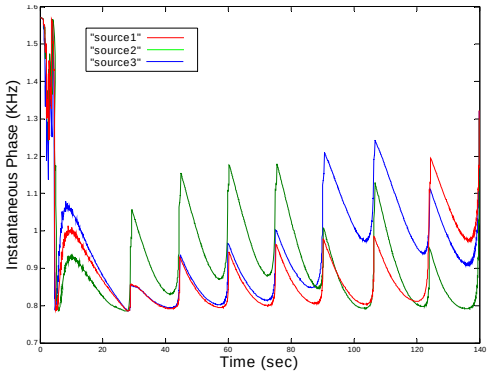


Fig.7. the instantaneous phase of three sources under Vegas

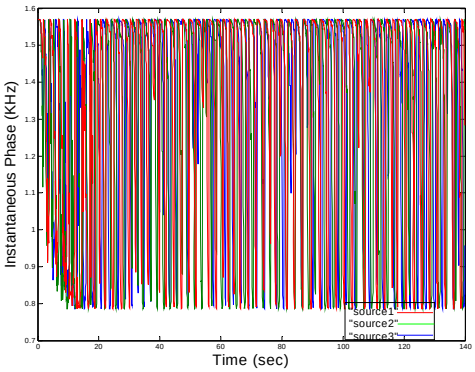


Fig.8. The instantaneous phase of three sources under Fast

4. CONCLUSIONS

In this paper the method of instantaneous phase and frequency is presented. We use different protocols to test our method. We propose a new method to express the window update. Using our method the congestion window can be changed to avoid synchronous. Our simulation result shows that, it really improves the frequency synchronization and the utilization of the bandwidth.

REFERENCES

[1] Michael Rosenblum. “Phase synchronization of chaotic systems:From theory to experiment application.”

[2] Joydeep Bhattacharyaa, Hellmuth Petscheb, Ute Feldmanna, Brigitte Rescherb. “EEG gamma-band phase

synchronization between posterior and frontal cortex during mental rotation in humans."

[3] Michael G. Rosenblum, Arkady S.Pikovsky, and J$\ddot{u}$rgen Kurths. "Phase Synchronization in Driven and Coupled Chaotic Oscillators."

[4] A.S.Pikovsky. "Phase synchronization of chaotic oscillations by a periodic external field," *Sov.J.Commun. Technol.Electron*.,vol.30,pp.85,1985.

[5] Michael G.Rosenblum,Arkady S.Pikovsky, and J$\ddot{u}$rgen Kurths. "Phase Synchronization of Chaotic Oscillators."

[6] Van Jacobson, Michael J.Karels. "Congestion Avoidance and Control," November 1988.

[7] Johanna Antila, "TCP Performance Simulations Using Ns2".

[8] RFC 2001 - TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms.

[9] Carl-Fredrik Westin. "A Tensor Framework for Multidimensional Signal Processing." Department of Electrical Engineering Link¨oping University, S-581 83 Link¨oping, Sweden Link¨oping 1994.

A MAODV_Based QoS Routing Protocol for Mobile Ad Hoc Networks*

Feng Zheng [1,2], Layuan Li [1], Jin Lian [1], Yefang Gao [1]
[1] School of Computer Science, Wuhan University of Technology
Wuhan 430063, P.R.China
[2] Department of Information and Command Automation, Air Force Radar Academy
Wuhan 430019, P.R.China

ABSTRACT

The study in mobile ad hoc networks results in many MANET's multicast routing protocols. This paper describes the multicast routing problem with QoS constraints, multicast ad hoc on-demand distance vector protocol (MAODV), and a network model for researching the Ad Hoc network QoS multicast routing problem. It presents a MAODV_based QoS routing protocol for mobile Ad Hoc networks(MAODVQ). Simulation results show that it is an available approach to multicast routing decision with QoS constraints.

Keywords: Mobile, Ad Hoc networks, Multicast, Quality of service (QoS), Protocol

1. INTRODUCTION

A mobile ad hoc network is a self-organizing network without any existing fixed communication infrastructure support or centralized control. As multimedia- and group-oriented computing becomes increasingly popular for the users of wireless mobile networks, the importance of features like quality of service (QoS) and multicasting support grows. Because of its independence of a fixed infrastructure and its instant deployment and easy reconfiguration capabilities, the ad hoc wireless networking technology shows great potential and importance in many situations, such as in military and disaster-relief applications. Some routing protocols for mobile Ad Hoc networks, such as AODV, DSR, MAODV etc. [1][2], are designed without explicitly considering quality of service of the routes. QoS routing in Ad Hoc networks has been studied only recently. QoS routing requires not only to find a route form a source to a destination, but the route must satisfy the end-to-end QoS requirement, such as bandwidth, delay and delay jitter etc. Quality of service is more difficult to guarantee in Ad Hoc networks than in other type of networks, because the wireless bandwidth is shared among adjacent nodes and the network topology changes as the nodes move. This requires extensive collaboration between the nodes, both to establish the route and to secure the resources necessary to provide the quality of service. This paper describes the multicast routing problem with QoS constraints, multicast ad hoc on-demand distance vector protocol (MAODV), and a network model for researching the Ad Hoc network QoS multicast routing problem. A MAODV_based QoS routing protocol for mobile Ad Hoc networks(MAODVQ) is presented. Its efficiency and robustness in mobile networks make it a good choice for mobile ad hoc networks.

2. QOS NETWORK MODEL

A mobile ad hoc network is usually represented as a weighted digraph G = (V, E), where V denotes the set of nodes and E denotes the set of communication links connecting the nodes. |V| and |E| denote the number of nodes and links in the network, respectively, Without loss of generality, only digraphs are considered in which there exists at most one link between a pair of ordered nodes [3][8].

Let $s \in V$ be source node of a multicast tree, and $M \subseteq \{V-\{s\}\}$ be a set of end nodes of the multicast tree. Let R be the positive weight and R^+ be the nonnegative weight. For any link $e \in E$, we can define the some QoS metrics:

delay function delay (e):$E \rightarrow R$
cost function cost (e): $E \rightarrow R$
bandwidth function bandwidth (e): $E \rightarrow R$
delay jitter function delay-jitter (e): $E \rightarrow R^+$

Similarly, for any node $n \in V$, one can also define some metrics:

delay function delay (n): $V \rightarrow R$
cost function cost (n): $V \rightarrow R$
delay jitter function delay-jitter (n): $V \rightarrow R^+$
packet loss function packet-loss (n): $V \rightarrow R^+$

We also use T (s,M) to denote a multicast tree, which has the following relations:

$$1) delay(p(s,t)) = \sum_{e \in p(s,t)} delay(e) + \sum_{n \in p(s,t)} delay(n)$$

$$2) cost(T(s,M)) = \sum_{e \in T(s,M)} cost(e) + \sum_{n \in T(s,M)} cost(n)$$

$$3) bandwidth(p(s,t)) = min\{bandwidth(e), e \in p(s,t)\}$$

$$4) delay-jitter(p(s,t)) = \sum_{e \in p(s,t)} delay-jitter(e) + \sum_{n \in p(s,t)} delay-jitter(n)$$

$$5) packet-loss(p(s,t)) = 1 - \prod_{n \in p(s,t)} (1 - packet-loss(n))$$

where p (s,t) denotes the path from source s to end node t of T (s, M). With QoS requirements, the problem can be represented as finding a path P*, such that

$$1) \prod_{l \in P^*} p_l(W) \geq \prod_{l \in P} p_l(W)$$

where $l \in E$ are the links in the path and $p_l(W)$ is the probability that the link l can accommodate a flow which requires w units of bandwidth.

$$2) \prod_{l \in P^*} p_l(\delta) \geq \prod_{l \in P} p_l(\delta)$$

where $p_l(\delta)$ is the probability that delay for link l is less than δ.

3. MAODV ROUTING PROTOCOL

Multicast ad hoc on demand distance vector (MAODV) routing protocol [2] is derived from AODV. The multicast

* This work is supported by National Natural Science Foundation of China (No. 60672137)

group leader maintains a group sequence number and broadcasts it periodically to keep fresh the routing information. A node wishing to join a multicast group generates a route request. Only the leader or members of the multicast group may respond to a join request by unicasting a route reply back to the requester, which selects the best from several replies in terms of highest sequence numbers and lowest hop count, and enables that route by unicasting a multicast activation message to its next hop. Intermediate nodes receiving the activation message unicast it upstream along the best route according to the replies they received previously. Nodes wishing to leave a group unicast a multicast activation message to their next hop with its prune flag set. Fig.1 shows how to join a node.

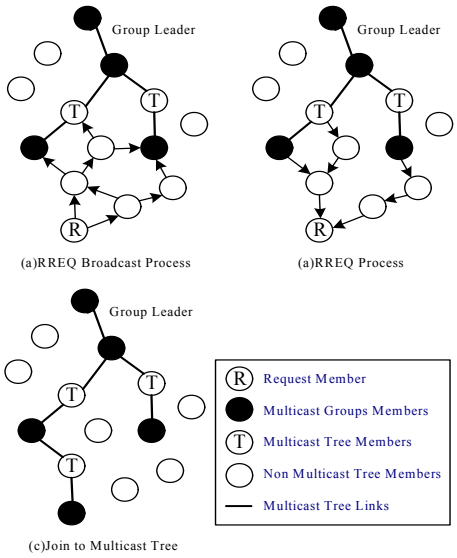


Fig.1. A Node Join Process

4. MAODVQ ROUTING PROTOCOL

MAODVQ Routing Protocol is an extension of MAODV protocol. It combines information from both the network and data link layer. Unlike other protocols which make QoS constraints calculations only after paths to the destination have been discovered [3-6], MAODVQ incorporates path finding with the QoS constraints reservation mechanism. MAODVQ is fully aware of the QoS constraints re-source availability by coupling together routing and MAC TDMA layers. As described earlier, the nodes compete for the slots contained in the data phase of the TDMA frame. In order for the source node to send data to a destination node, it must establish a virtual circuit connection with that destination. The virtual circuit establishment process includes route discovery, QoS constraints calculation and reservation components. Each node keeps a schedule which contains information about both its own and its neighbor's time slots that are used for sending and receiving. The paper in [4] includes the algorithm used by each node to determine which slots are available to send to and receive from its neighbor, and to calculate link QoS constraints scheduling from itself to each of its neighbors.

For example, the link bandwidth information is used in the calculation of the path bandwidth schedules to source and destination nodes. Modified MAODV HELLO messages are used which include slot scheduling information. The HELLO messages are sent either periodically or when link bandwidth information is changed. In MAODVQ, path discovery is done in the following manner. A source node that wants to send data to a particular destination determines if it has enough link bandwidth available to any of its neighbors. If it does not, it then denies the request initiated by its application layer. When an intermediate node receives a RREQ message, it checks whether it already has an entry in its routing table corresponding to the received application. The node then calculates the path bandwidth schedules using algorithms similar to ones presented in [7]. If the calculated path bandwidth to the source is insufficient, then the node does not forward the RREQ message. Otherwise, the intermediate node augments the RREQ message with path and link bandwidth parameters and broadcasts it further. The link bandwidth between two nodes is calculated as the intersection of their free slot schedules. The send link bandwidth is defined as the intersection of the free send slot schedule of the sender node and the free receive slot schedule of the receiver node. The receive link bandwidth is defined as the intersection of the free receive slot schedule of the receiver node and the free send slot schedule of the sender node. Fig.2 shows MAODVQ packet.

Type	length	QoSObject

Fig.2. MAODVQ packet

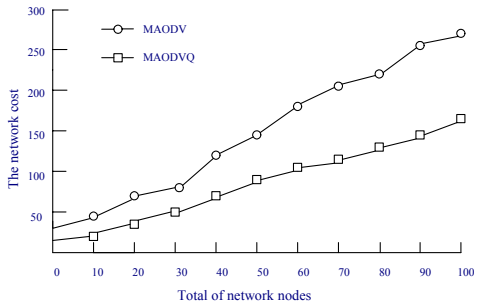
5. SIMULATIONS

We conduct simulations to evaluate MAODVQ, MAODVQ is implemented by using the Network Simulator (NS) and its performance is compared with MAODV routing protocol. The network graphs used in the simulations are constructed by the Waxman's random graph model [5]. In this random graph, the edge's probability can be

$$p_e(u,v) = \beta \exp(-\frac{d(u,v)}{aL})$$

where d (u,v) is geometric distance from node u to node v, L is maximum distance between two nodes, parameter a can be used to control short edge and long edge of the random graph, and parameterβcan be used to control the value of average degree of the random graph.

In the simulation, the nodes are uniformly distributed all over the region. Nodes in the simulation move according to "random waypoint" model. The mobility speed of a node is set from 0m/s to 30m/s. The 50 nodes randomly distribute in 1km×1km. The transmitting radius of each node is about 250 meters and channel capacity is 2Mbps. Fig.3 shows the contrast of the network cost , data transmission rate and finding path success rate between MAODV and MAODVQ.



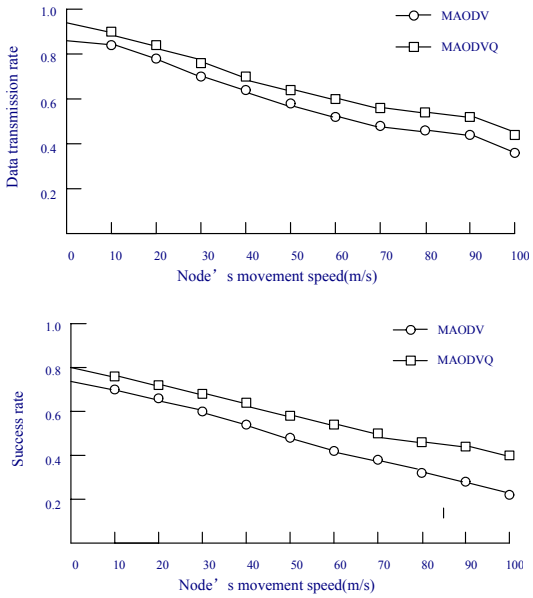


Fig.3. Contrasts between MAODV and MAODVQ

6. CONCLUSIONS

In this paper, a MAODV_based QoS routing protocol for mobile Ad Hoc networks(MAODVQ) is presented. In contrast with Multicast Ad Hoc on demand distance vector (MAODV) routing protocol, MAODVQ has produced significant improvements in data transmission rate, finding path success rate and network cost. Its efficiency and robustness in mobile networks make it a good choice for mobile ad hoc networks. The studies show that MAODVQ can provide an available approach to QoS multicast routing for mobile Ad Hoc networks. Our future work includes a performance evaluation of the MAODVQ in realistic simulation environments.

REFERENCES

[1] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das. "Ad Hoc On-demand Distance Vector Routing," October 99 IETF Draft.

[2] Royer, E.M, and C.E. Perkins, "Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing," *IETF MANET WG Internet Draft, work in progress*, July 2000.

[3] Y.-K. Ho and R.-S. Liu, "On-demand QoS-based Routing Protocol for Ad Hoc Mobile Wireless Networks," *Fifth IEEE Symposium on Computers and Communications,* 2000. Proceedings. ISCC 2000, July 2000,pp. 560–565.

[4] I. Gerasimov and R. Simon, "A bandwidth-reservation mechanism for on-demand ad hoc path finding," *IEEE/SCS 35th Annual Simulation Symposium*, San Diego, CA, April 2002, pp. 27–33.

[5] B. M. Waxman, "Routing of Multipoint Connections," *IEEE Journal of Selected Area in Communications*, Dec. 1998, pp. 1617–1622.

[6] C. R. Lin and C. C. Liu, "An on-demand QoS routing protocol for mobile ad hoc networks," *Conference on IEEE International Networks, (ICON 2000) Proceedings*, Spetember 2000, pp. 160–164.

[7] C. R. Lin and J. S. Liu, "QoS routing in ad hoc wireless networks," *IEEE Journal on selected areas in communications*, August 1999, pp. 1426–1438.

[8] Li Layuan, Li Chunlin, "A Hierarchical QoS Multicast Routing Protocol for Mobile Ad-Hoc Networks," http://www.paper.edu.cn/lilayuan1.pdf

Feng Zheng is a Ph.D. student of Computer Science and Technology, Wuhan University of Technology. He graduated from Wuhan University of Technology in 1983, from National University of Defense Technology in 2001 with specialty of pattern recognition. He is an associate professor of Computer Science, Air Force Radar Academy. His research interests are in mobile ad hoc network routing protocol, network security and software development method.

A Rate-based Congestion Control Mechanism for Streaming Media*

Peijuan Qu [1], Mingli Wei[2], Qiuyu Zhang[3]
College of Computer and Communication, Lanzhou University of Technology
Lanzhou, Gansu, China
Email: weimingli7861@126.com

ABSTRACT

An ameliorated algorithm of TFRC is proposed by learning the basic mechanism of TFRC in this paper. The ameliorated algorithm colligates modified tfrc throughput equation and the policy of matching the average receive-rate to the average of the send-rate. By matching the actual and expected receive-rates, congestion can often be detected before packet losses occurring. It can help to avoid packet losses and stabilize the transmission rate quicker at session start-up. The application of the modified tfrc throughput equation can estimate the available bandwidth more accurately and improve the smoothness of the streaming media significantly. Simulation on NS2 verifies the validity of our algorithm. Comparing to TFRC, the ameliorated algorithm shows a better performance of real-time and smoothness. And it also has a good convergence time and less packet losses.

Keywords: Streaming Media, Congestion Control, TCP-Friendly TFRC.

1. INTRODUCTION

With the rapid developments of wide bandwidth networks and high performance Computers, more and more multimedia real-time applications are applied in Internet, such as digital libraries, distant learning and shopping etc. Thus they require isochronous processing and quality-of-service (QoS) from the end-to-end point of view. TCP is ill-suited to real-time flows because of its high variation of sending rate. So the UDP is used in nowadays network to transport real-time application. Since UDP does not implement congestion control, protocols or applications that are implemented using UDP should detect and react to congestion in the network. S.Floyd put forward TCP-friendly Rate Control (TFRC)[1-3]. He pointed out that congestion control should be added in the transport protocol for real-time multimedia applications in order to make them friendly to TCP flows. That means when congestion occurs, real-time flow can compete for bandwidth with TCP in a fair manner.

In this paper, we study the basic mechanism of TFRC, and present a ameliorated algorithm of TFRC. The ameliorated algorithm colligates modified tfrc throughput equation and the policy of matching the average receive-rate to the average of the send-rate.

2. SUMMARY OF TFRC

2.1 Algorithm of TFRC

TFRC is a rate-based, end-to-end congestion control protocol which is intended for unicast playback of Internet streaming applications. The sender uses the slow start technique at the beginning of the transmission phase, during which it tries to increase its sending rate multiplicatively at every RTT until it detects a loss**.** Packet losses are identified by gaps in the sequence number of the transmitted packet at the receiver module. The receiver measures the packet loss rate and feeds this information back to the sender at regular intervals. Then the sender uses the feedback information to measure the RTT to the receiver.

In order to derive an acceptance TCP-friendly transmission, the TFRC sender adjusts its transmission rate based on the measured loss rate and RTT**.** The adjustment of the sending rate to achieve TCP-friendliness is based upon a control equation derived from the TCP throughput model[4].The throughput equation is as follows:

$$R = \frac{s}{RTT \times \sqrt{\frac{2bp}{3}} + RTO \times \sqrt{\frac{3bp}{8}} \times p \times (1 + 32p^2)} \quad (1)$$

R: the transmit rate in bytes/second. s*:* the packet size in bytes. RTT: the round trip time in seconds. p*:* the loss event rate, between 0 and 1. RTO: the TCP retransmission timeout value in seconds, generally, RTO = 4RTT. b: the number of packets acknowledged by a single TCP ACK.

The transmission rate of the sender is adjusted directly to match the calculated transmission rate. The rate adjustment process is made periodically at a certain interval. In the event of packet losses, the sender restricts its sending rate to the equivalent TCP rate by using throughput equation. Otherwise, the transmission rate is doubled.

2.2 Problems Exited in TFRC

(1) Seen from the above throughput equation, the overall rate change is proportional to $1/p\sqrt{p}$. Such proportionality makes rate change still over sensitive to packet losses, especially when packet loss ratio is small.

(2) Even if the channel bandwidth is a constant, TFRC cannot stay at constant bandwidth at its steady state. Instead, it still tries to increase the sending rate over constant bandwidth, which unfortunately leads to a short-term congestion.

(3) TFRC responds slower to losses than TCP does, and increases the send-rate much slower during loss-free periods[5] .

3. ALGORITHM OF AMELIRATED TFRC

3.1 Modified Tfrc Throughput Equation

According to the above analysis, improvement is to set the derivative of R to $1/p$ instead of $1/p\sqrt{p}$. The modified tfrc throughput equation[6] is as follows:

$$R = \frac{s}{RTT}[\sum_{n=0}^{\infty} a_n \log^n(p)] \quad (2)$$

In the paper, we use a simple one. It is as follows:

$$R = \frac{s}{RTT}[a_0 + a_1 \log(p)] \quad (3)$$

Now we calculate a_0 , a_1. For the practical media streaming transmission over the Internet, we can make s = 1 K bytes, RTT

* The Natural Science Foundation of Gansu (3ZS062-B25-033)

= 100ms and assume that transmission has no effect when packet loss becomes large. For example, when p>60%, R=0, we set the desired throughput at p = 0.1% and calculate a_0 , a_1.

Hence, the throughput formula becomes

$$R = \frac{k}{RTT}[-0.25 - 0.5\log(p)] \quad (4)$$

Where k is a control parameter. In order to keep TCP-friendliness, we can set k=8.

In the next policy of matching the average receive-rate to the average of the send-rate ,we use the modified tfrc throughput equation (4) instead of the primary throughput equation (1).

3.2 The Policy of Matching the Average Receive-rate to the Average of the Send-rate[7]

In case of TFRC, the sender includes its current send-rate at the time of transmission in each data packet. The send-rate reported in packet i is denoted by Xi in the TFRC specification1[8].

The average of the send-rates R_i is reported in the data packets during a measurement interval. The receiver can infer the average of the send-rate over the measurement interval from the values of R_i contained in the TFRC data packets as follows: Let T_{recv} be the length of the measurement interval, in standard TFRC, T_{recv} equals one RTT, and n is the number of packets received during that interval. The packets are numbered 1,…,n, and contain the respective send-rates R_1 , R_2 …, R_n . When sending packets at a rate R, the sender will schedule packets such that a packet is transmitted every $1/R$ seconds. Thus, the time interval between the transmission of two consecutive packets i and i+1 is $1/R_i$ seconds. The total time required by the sender to send a series of packets 1,…,n is $T_{send} = \sum_{i=1}^{n} 1/R_i$.

The average send-rate during that interval is $R_{send} = \frac{n}{T_{send}}$.

The measured average receive-rate is $R_{recv} = \frac{n}{T_{recv}} = \frac{n}{RTT}$.

If the transmission is not limited by the available bandwidth, average send-rate and the measured average receive-rate are equal at the time of arrival at the receiver. On the other hand, the available bandwidth limits the transmission speed, some of the packets will be spread out in time and the average receive-rate will stay behind the average send-rate.

Calculate the R_{diff} , which is the difference between R_{recv} , R_{send} , $R_{diff} = R_{send} - R_{recv}$.

If $R_{diff} > \alpha R_{send}$, perform the next two steps:

a. Calculate the approximate TFRC loss interval corresponding to R_{recv} , and insert a synthetic loss interval of this length into the loss history.

b. Immediately send a feedback report containing the resulting loss rate to cause the TFRC sender to leave slow-start and adjust the rate close to R_{recv} .

How to decide parameter α ? On one hand, it should be tolerant enough to not terminate the slow-start prematurely because of small fluctuations in the transmission rate or imprecise packet scheduling by the sender. On the other hand, it should detect as quickly as possible when the receive-rate starts to deviate from the send-rate to improve our chances to react before the first packet losses occur. In the simulation α = 0.1

4. SIMULATION RESULTS

We use NS-2.28[9] as our simulator .In the experiment , we use the typical dumbbell topology.

(1) Performance of real-time

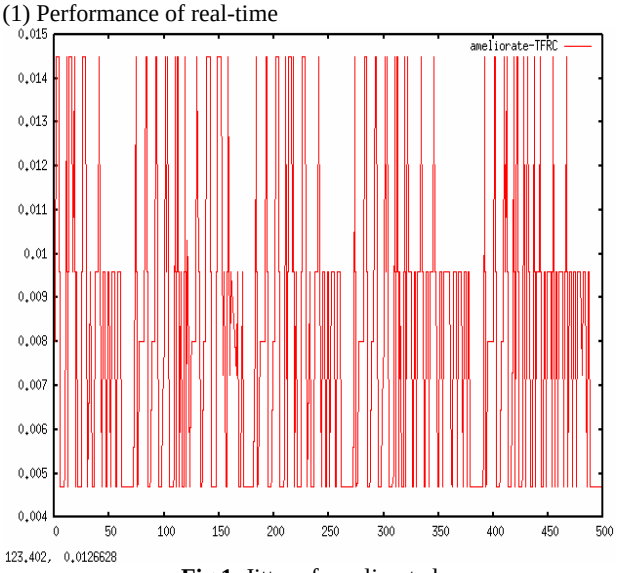


Fig.1. Jitter of ameliorated

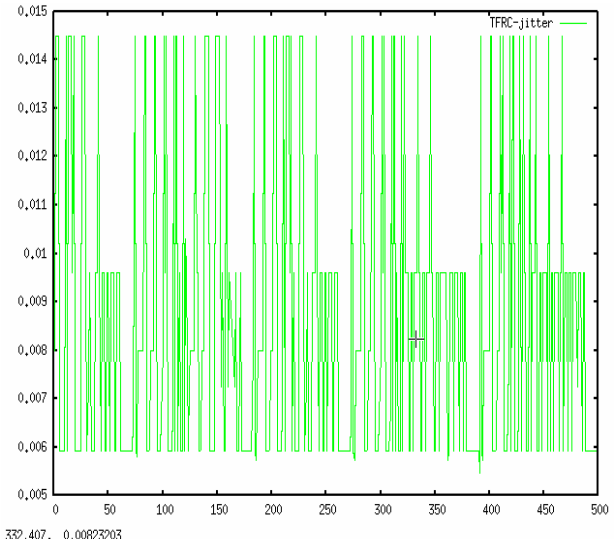


Fig.2. Jitter of TFRC

Fig.1 and Fig.2 show the jitters of TFRC and ameliorated TFRC. We can see that the average jitter of ameliorated TFRC is lower than TFRC's jitter. So ameliorated TFRC is more suitable to real-time streaming media.

(2) Performance of smoothness

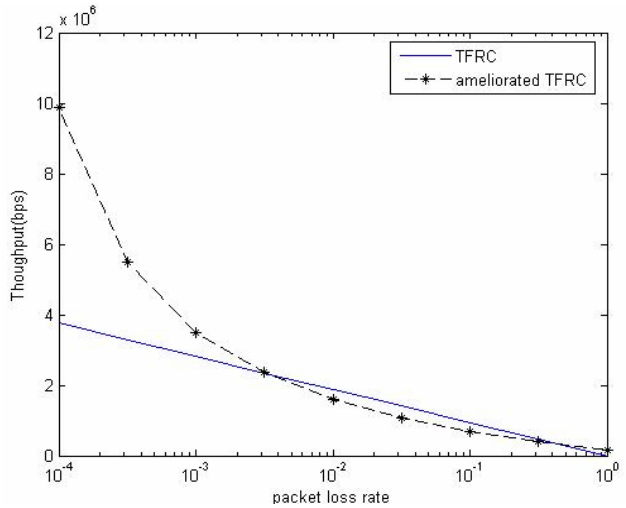


Fig.3. Throughputs of TFRC and ameliorated TFRC

As seen from Fig.3, Ameliorated TFRC changes slower in low packet loss ratio case, f aster in high packet loss case. So ameliorated TFRC has more smoothness than TFRC.

(3) Convergence time and packet losses

Table 1 below sums up the convergence time and packet losses, when queue size is 15 packets.

Table 1. Convergence Time and Packet Losses

	Packet Losses	Convergence Time
TFRC	34	24.43s
Ameliorated-	1	24.21s

5. CONCLUSIONS

The ameliorated algorithm colligates modified tfrc throughput equation and matches the average receive-rate to the average of the send-rate policy. In the algorithm, the receiver can update its send- rate and receive-rate estimates for every arriving packet, while a sender-based scheme would have to rely on receiver feedback to determine the receive-rate. In protocols such as TFRC that do not use per-packet acknowledgments, feedback reports are sent relatively infrequently. Thus, the receiver-based approach has the potential to allow for a quicker detection of rate mismatches. Using the modified tfrc throughput equation can improve the smoothness of the streaming media significantly Compared to TFRC, the ameliorated algorithm show a better performance of real-time and smoothness, and has a good convergence time and less packet losses..

REFERENCES

[1] Floyd S, Handley M, Padhye J, et al. ”Equation-based Congestion Control for Unicast Applications.” ACM SIGCOMM, 2000.

[2] Floyd S, Handley M, Padhye J, et al. ” Equation-based Congestion Control for Unicast Applications,The extended version.” ICSI Technical Report TR-00-03, URL.

[3] Floyd S, Handley M, Padhye J and J.Widmer,”TCP friendly rate control:Protocol Specification”,January 2003,*Network Working Group RFC* 3448.

[4] J. Padhye, V. Firoiu, D. Towsley, J. Kurose: Modeling TCP Throughput.

[5] D. Bansal, H. Balakrishnan, S. Floyd, S. Shenker: Dynamic Behavior ofslowly-Responsive Congestion Control Algorithms, SIGCOMM 2001.

[6] Zhen Li, Guobin Shen, Shipeng Li, EdwardJ. Delp,” L-TFRC:An end-to-end congestion control mechanism for video streaming over the internet**”** IEEE ICME ,2003.

[7] Stephan Baucke,”Using Receiver-Based Rate Matching for congestion detection in Rate-Based protocols” IEEE ,2003.

[8] M. Handley, J. Pahdye, S. Floyd, J. Widmer: TCP Friendly Rate Control (TFRC): Protocol Specification, Internet Draft, work in progress,October 2002.

[9] NS Web Page: http://www.isi.edu/nsnam.

Peijuan Qu: Higher Engineer, Dean of Science office of School of Computer and Communication, Lanzhou University of Technology, Mrs Qu is always engaged in the laboratory work of computer and communication, her research interests include: signal processing, multimedia communication, etc.

Mingli Wei, student of master. Born in Huaibei .Anhui province in 1984, she has published some academic papers .Her research interests include: multimedia communication, the control of quality of service in the transmission of streaming media.

Research and Implementation of Network Performance Management System

Nengli Zhang [1] , Erpeng Zhu [2], Xiaoping He, Fengling Guo, Yaguo Fan, Mingjun Chen
(School of Computer Science and Technology,
Wuhan University of Technology,Wuhan Hubei 430070,China)
Email:zhangnl@whut.edu.cn, whzl666@163.com

ABSTRACT

This paper introduces the system architecture and the software implementation of network performance management system based on NetFlow protocol, and then discusses the storage technologies of the network massive information and the network traffic rank algorithm. Finally, the paper introduces the functions of the present system and the goals to work for next.

Keyworks: NetFlow, Berkeley DB, JudyArray, Red-Black Tree

1. INTRODUCTION

With the development of network applications, the structure of the network system becomes more and more complex, and the scale becomes larger and larger, so the network system objectively needs network performance management software to ensure the system to operate normally. Real-time monitoring and managing the network system, host systems and application systems, and Network Performance Management System can provide many functions and services such as real-time monitoring and performance analysis of the network and application system, SLA service quality management, fault diagnosis and capacity planning. On the basis of collection and analysis of the network meta-information, Network Performance Management System can summarize and merge the information, and then display the real-time performance status about the certain network in the chart.

2. NETWORK MANAGEMENT PROTOCOL

The network meta-information comes from the network equipments such as router or switcher. And when these devices process the function of transmission, they also send the relevant network flow information, which is the meta-information in the paper, according to the current configuration of the device themselves. The information are generally attached to the following popular network management protocols: Simple Network Management Protocol(SNMP), Remote Monitoring (RMON), NetFlow, and sFlow. Among them, NetFlow is a data packet switching technology defined by Cisco and it can be used to record flow information at the same time[1].

Currently, the research on NetFlow protocol is mainly based on the V5 version of NetFlow protocol[2].As NetFlow(V9) is the latest version of Cisco's Network Management Protocol, so the core software of Network Perfermance Management System discussed in this paper is based on NetFlow (V9) protocol and is achieved on the Linux platform in the C language.

3. NETWORKPERFORMANCE MANAGEMENT SYSTEM ARCHITECTURE

The system hardware is composed of Information Collector,Remote Probe（Prob）,Database Server and Web Server. The network information collector can receive data packets that come from NetFlow, SFlow and SNMP, and Remote Probe（Prob）can collect the information that comes from devices that do not support NetFlow and SFlow. If we consider Server, Information Collector, Database Server and Web Server actually a device, to make clear the hardware architecture, we will separate them in the next picture.

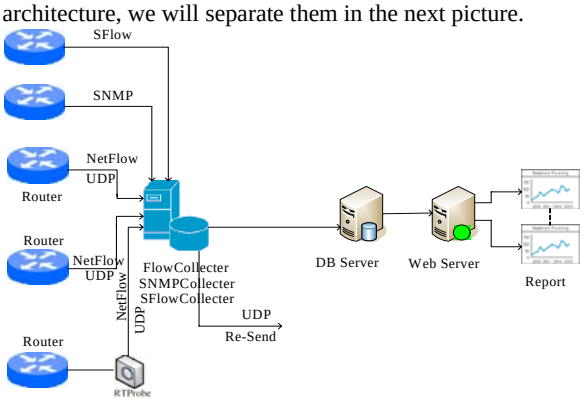


Fig.3-1. Hardware structure of the system

4. SOFTWARE DESIGN OF NETWORK PERFORMANCE MANAGEMENT SYSTEM

The software is mainly composed of the information receiver module, the Bekeley DB massive storage module, the relational database module, the network performance analysis module and the data-showing module. And the information receiver module is composed of NetFlow receiver module, SNMP receiver module and SFlow receiver module. This paper mainly describes the implementation of NetFlow receiver module. [3]

4.1 The structure and function of NetFlow receiver module

Fig.4-2 shows the structure of NetFlow receiver module. The module uses a process to receive NetFlow data packets and multiprocessors to write the received NetFlow data packets into Berkeley Database. Among them, IPC message queue is used for storing the received NetFlow data packets. ShMem shared memory is used for storing some statistical information.

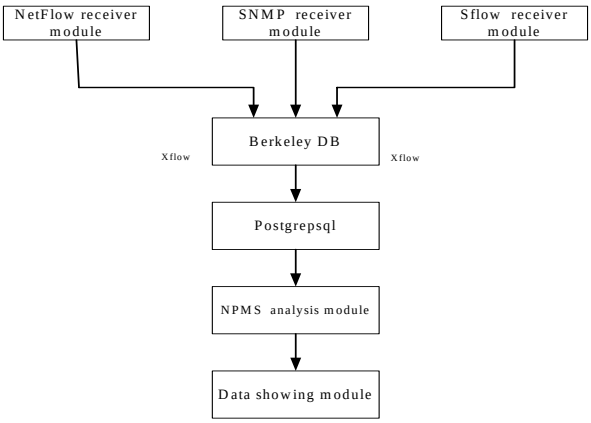


Fig.4-1. Software structure of the system

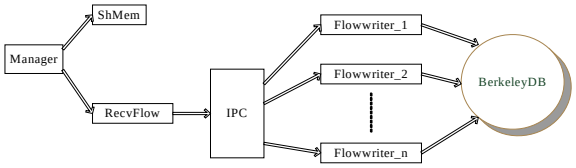


Fig.4-2. The structure chart of NetFlow receiver module

4.2 The Massive Network Data Processing

According to statistics, the average transmission rate of the NetFlow flow data generated by the single router is 1,500 flows per second. If this average value is used in calculation, we can obtain 5,400,000 flows per hour and 129,600,000 flows per day. We can see that there are about 130 million flows of NetFlow original records and 8G (68 x 130 million) data a day. Therefore, how to design a highly effective processing subsystem of massive information is one of the key questions in implementing Network Performance Management System.

4.2.1 The Network Massive Data Storage

Because the network information processing needs resolving the massive and real-time questions and the general relational database is not a component, so the system uses Berkeley DB embedded database to store the flow information. Berkeley DB can include certain records, and each record is composed of the keyword and data (key/value) which may be a simple data type and a complex data type.

Berkeley DB has four access methods: Btree, Hash, Queue and Recno. The type of the key of Queue and Recno is an integer and the key of Btree and Hash is a complex type. To select an access method, you should first consider the actual data type of the key, and then you should consider the performance influence of this access method. To improve the speed in this case, we choose the Queue method.

In BerkeleyDB, we can query database only by the key value; that is to say there is only the key index in BerkeleyDB. In this model, we use the data of the NetFlow type as the data of the primary database and use all fields of the NetFlow type to build secondary databases. The following is a part of the key code involved in operating the database:

```
/* Env structure handle */
DB_ENV  *myEnv;
/* DB structure handle */
DB **primary_db;
 /* Set env open flags support shared memory support
    transaction support logging support locking*/
 u_int32_t env_flags = DB_CREATE | DB_INIT_MPOOL |
                       DB_INIT_TXN  |  DB_INIT_LOG
                       |DB_INIT_LOCK;
/* Create an environment handle */
db_env_create(&myEnv,0);
 /* Set the environment cache size. The cache can first save
    some data in memory then save them in hard disk when
    apparently transferring flush or close function. It can
    improve the performance of operating database */
myEnv->set_cachesize(myEnv,0,128*1024*1024,0);
 /*According to environment flags open the environment in
    the special directory and multi-database can share an
    environment */
myEnv->open(myEnv,conf->flowd_data_path,env_flags,0);
/* Create a primary handle in the environment */
ret = db_create(primary_db, myEnv, 0);
/* ? Set the underlying database page size. If setting the page
size is illogical, it maybe influence the performance of
operating database, so generally set the page size by the size of
OS page layout        */
 int pagesize =4096;
 (*primary_db)->set_pagesize(*primary_db, pagesize);
 /* Set the database cache size */
 (*primary_db)->set_cachesize(*primary_db,  0,  5000  *
pagesize, 0);
  /* Set the length of the data stored in the database when
     using Queue access method ,and set the length by the
     bytes of xflow record body */
 (*primary_db)->set_re_len((*primary_db),sizeof(xflow));
 /* Rename the primary database */
 asprintf(&primary_db_name, "%s%s", db_name, ".db");
 /* Open database */
 (*primary_db)->open((*primary_db),          NULL,
primary_db_name, NULL, DB_QUEUE, DB_CREATE, 0);
```

Actually each database is a table in Berkeley DB, the so-called secondary database is very similar to the index of relational database, so it can improve the efficiency of information retrieval based on specific key value. According to our business needs, we have established five secondary databases, which respectively are five fields of the NetFlow flow structure including ipv4_srcaddr（the source IP address）, ipv4_dstaddr(the destination IP address) , srcport (TCP/UDP source port or equivalence), dstport (TCP/UDP port or equivalence) and endtime (SysUptime when the last packet of the flow is received).Therefore when we use these fields to take the corresponding network flow information from Berkeley DB, the efficiency becomes better.

4.2.2 The Ranking Algorithm of Network Traffic

For Network Performance Management System, it is the basic function to be ranked by traffic for IP address(TopN).As IPV4 addresses are 32-bit, if we use the fixed array, it needs the space of 16G memory. But it is clearly unrealistic. And it is not true that each IP address has traffic for a router in a certain period of time, so it is not necessary to assign array in the fixed IP address. In this system, we use the JudyArray invented by Doug Bakins to achieve the traffic increments in IP address, and then use the Hash Red-Black Tree to achieve the dynamic traffic rankings in IP address. In most cases, the accessing speed of the JudyArray is comparable to the visit speed of the Hash Algorithm, and it is much faster than algorithm based the tree structure. In contrast, the memory consumption is much smaller than Hash and tree structure in large-scale data processing. [4]

To improve the speed of data access and reduce memory consumption, we use the JudyArray array as cache and process one-minute data convergence in the JudyArray, then process the TOPN ranking when the converged data enter the corresponding Hash Red-Black Tree. The entire data flow is shown in Fig.4-3. [5]

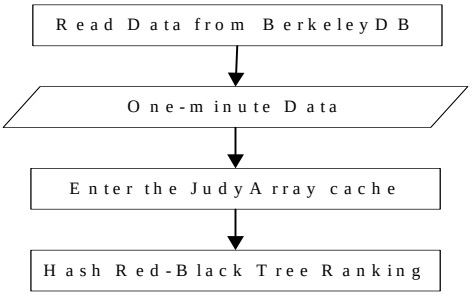


Fig.4-3. Algorithm of data processing

5. CONCLUSIONS

This system runs under the Linux operating system; the server configuration is CPU 2GHz and the memory is 2G. In the test, we send the NetFlow packets by a constant speed of 10,000 flow per second to the server and implement the traffic ranking in the region, the destination IP, the source IP, the protocol and the session, and show the real-time dynamic ranking through the Web method. We expect to achieve a goal that our system can complete the above work in 30 seconds and the memory consumption rate is always controlled below 10% .The system has realized the NetFlow network flow data reception and the real-time dynamic sorting by network traffic, but has not yet achieved abnormal behavior analysis, which is our target of next stage.[6]

REFERENCES

[1] Cisco IOS NetFlow Technology Data Sheet, online at http://www.cisco.com/netflow.

[2] Bo Yang, "A Flow-based Network Monitoring System Used for CSCW in Design"，*Proceedings of the Ninth International Conference on* Volume 1, 24-26 May 2005 Page(s):503 - 507 Vol. 1.

[3] http://berkeleydb.net/man/bdb/index.html.

[4] http://judy.sourceforge.net/.

[5] Zhou Wei Ming，*Data Structure and Algorithm In Muti-Task*, Publisher of Huazhong University of Science & Technology，April 2006.

[6] Tang-Long Pao, "NetFlow Based Intrusion Detection System", *Proceedings of the 2004 IEEE International Conference on Networking*, Sensing & Control Taipei. Taiwan, March 21-23, 2004.

Nengli Zhang is a vice professor working at School of Computer Science and Technology, Wuhan University of Technology. He graduated from Wuhan University in 1991. His research interests are network security, dynamic web technology and e-commence.

A New Analytic Queuing Model with Self-Similar Input Traffic *

Gongchao Su, Xiaohui Lin, Hui Wang
College of Information Engineering, Shenzhen University
Shenzhen, Guangdong Province, P.R.China
Email: {gcsu, xhlin, wanghsz}@szu.edu.cn

ABSTRACT

The self-similar nature of high-speed network traffic has been widely recognized as a critical issue in understanding and evaluating network performance. In this paper we develop a new analytic queuing model, called the N-Burst/D/1 model, to reflect self-similar characteristics of real network traffic and its impact on network queuing systems. The self-similar input traffic is generated as N-Burst arrival process, and an analytic queuing analysis is presented to address network behavior in the context of high speed communication systems. We compare our results with traditional M/D/1 queuing model with Poisson arrival process. Our results indicate that the proposed model is more accurate to model real traffic in high-speed networks than traditional Poisson distribution models, and our theoretical calculation and extensive simulation also show that under certain network conditions queuing performance can be predicted to estimate realistic network performance.

Keywords: Queuing Theory, Self-Similarity, N-Burst, M/D/1 Queue

1. INTRODUCTION

It has been widely accepted that standard Poisson or Markovian processes do not adequately model network traffic[1].Recent studies in many literatures during the past decade show that network traffic, especially wide area network traffic, exhibits a so-called self-similar property. Such property has severe consequences on network behavior and has become a critical issue in evaluating network queuing performance such as packet delay, packet dropping and queue size estimation.

Queuing systems in high-speed networks are often modeled as G/D/1 queue, particularly M/D/1 queue with one service equipment and fixed service time distribution, which uses Poisson or Markovian processes to generate traffic. However, queuing analysis based on this model is not accurate to reflect real network performance, since it does not take into account the self-similar nature of network traffic.

A variety of stochastic processes have been proposed to model this behavior, such as FRP[2]，F-ARIMA[3]，FGN[4], etc. Compared with many other stochastic processes, the N-Burst arrival process proposed in [6] is more adaptable, accurate and implemental to model realistic network traffic [5-7].

Therefore, this paper choose the N-Burst arrival process to generate self-similar traffic and proposes the N-Burst/D/1 queue to model queuing systems in high speed networks. We present our queuing analysis of the N-Burst/D/1 queue and compare our results with the M/D/1 queue under similar network environments. We formulate our results and analyze network performance under dynamic network environments.

This paper is organized as follows. Section 2 describes the N-Burst arrival process. Section 3 introduces the N-Burst/D/1 queuing system and studies the queuing behavior. Section 4 presents extensive simulation in OPNET. We give our conclusion in Section 5.

2. THE N-BURST ARRIVAL PROCESS

Lipsky *et al* proposed the N-Burst arrival process in [6], which model network traffic as a supervision of N independent, identical ON/OFF sources. Each source sends packets based on Poisson process during ON period, and remains silent during OFF period. Durations of these two periods follow a Pareto distribution and an exponential distribution, respectively. The N-Burst process can be categorized as 1-Burst process and N-Burst process according to the number of sources.

1-Burst process contains only one ON/OFF source. The duration of ON period follows a Pareto distribution. For a stochastic variable s with Pareto distribution, its probability density function (PDF) can be described as:

$$f_1(s) = \alpha\beta^{\alpha} s^{-\alpha-1}, a > 0, \beta > 0 \quad (1)$$

Its probability function is:

$$F_1(s) = 1 - \left(\frac{\beta}{s}\right)^{\alpha}, s > \beta \quad (2)$$

α is the shape parameter and β is the location parameter. For a stochastic variable ϕ with exponential distribution, its PDF can be described as:

$$f_2(\phi) = \lambda e^{-\lambda\phi}, \phi \geq 0 \quad (3)$$

Its probability function is:

$$F_2(\phi) = 1 - e^{-\lambda\phi}, \lambda > 0 \quad (4)$$

During ON period the source generates packets at a rate δ. For N-Burst process, suppose that each source generate packets at an average rate κ, since each source is identical, the traffic sources generate packets at an average rate $C = N\kappa$ .If throughout time interval [0,t], there are i sources are simultaneously in their ON period, the sending rate can also be described as :

$$C_i = i \cdot \delta + (N - i) \cdot \kappa \quad (5)$$

3. THE N-BURST/D/1 QUEUE

In this part we propose the N-Burst/D/1 queuing model as illustrated in Fig.1. We consider an infinite buffer with FCFS (First Come First Serve) service discipline. Apparently, if the system has a fixed service rate C_0, for any incoming packet with a fixed length of M, the service time TS can be represented as $T_s = M / C_0$.

*This work is partially supported by the Natural Science Foundation of China(NSFC 60602066) and of Guangdong Province(5010494)

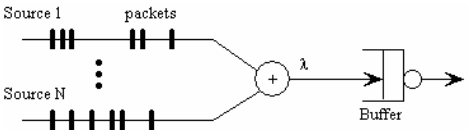


Fig.1. N-Burst/D/1 queuing system

According to Little's Formula [8], the average queue length $\overline{L}$ can be denoted as:

$$\overline{L} = \lambda \overline{W} \tag{6}$$

λ is the incoming rate, which is the source rate C of the N-Burst processes. $\overline{W}$ is the average waiting time.

To understand the performance of the queuing system, it is left to calculate the average waiting time. The rest of our discussion focuses on this issue.

3.1 Average Waiting Time in N-Burst/D/1 Queue

Assume the indicator random variable $I(t)$ is 1 if and only if the number of the sources that are simultaneously in their ON period does not change during the whole (0,t) period, otherwise $I(t) = 0$. $P_I(t)$ denotes the probability $P_I(t) = \Pr(I(t) = 1)$. The indicator random variable $I(i,t)$ is 1 if and only if exactly I sources are simultaneously in their ON period during (0,t) period. Otherwise I(i,t)=0. We denote $P_i(t) = \Pr(I(i,t) = 1)$. Note $P_I(t) = \sum_{i=0}^{N} P_i(t)$.

According to [7], if the queuing system is under low traffic load, the waiting time W(t) can be calculated as:

$$\begin{aligned} W(t) &= P_I(t) \cdot W(t \mid I(t) = 1) + (1 - P_I(t)) \cdot \\ W(t \mid I(t) = 0) &\cong P_I(t) \cdot W(t \mid I(t) = 1) \\ &= \sum_{i=0}^{N} P_i(t) \cdot W(t \mid I(i,t) = 1) \end{aligned} \tag{7}$$

And the average waiting time E(W(t)) satisfies:

$$E(W(t)) \cong E(\sum_{i=0}^{N} P_i(t)) \cdot E(W(t \mid I(i,t) = 1)) \tag{8}$$

Furthermore, to calculate the waiting time of our model it is left to calculate the waiting time of corresponding M/D/1 queue with the same input traffic rate. According to [8], the average waiting time of M/D/1 queue is:

$$E(W_1(t)) = \frac{T_s}{1-\rho} \cdot (1 - \frac{\rho}{2}), 0 < \rho < 1 \tag{9}$$

T_S is the service rate and ρ is the system utilization ratio, $\rho = C / C_0$.

From Eq.(8) and Eq.(9) we can conclude that the average waiting time of N-Burst/D/1 queue under low traffic load is:

$$E(W(t)) \cong E(P_I(t)) \cdot \frac{T_s}{1-\rho} \cdot (1 - \frac{\rho}{2}), 0 < \rho < 1 \tag{10}$$

Note that the average waiting time of N-Burst/D/1 queue is smaller than that of M/D/1 queue, since $E(P_I(t)) < 1$.

However, as system utilization ratio ρ increases and approaches 1, the N-Burst sources reaches a blow-up region, that is , according to [5], there will be very long bursts for some of the sources because of the heavy-tailed characteristics of N-Burst processes. The queue length q(t) follows a linear increase, $q(t) \sim (C_i - C_0)t$.

For any packet that enters the queue at time spot t, its waiting time w(t) can be denoted as:

$$w(t) = (q(t) + 1) / C_0 \tag{11}$$

That is to say, the average waiting time of the queue will be increasing almost linearly. We find that the queue length and average waiting time of the queue increase very drastically when ρ approaches 1 and this indicates that the performance of the queuing system deteriorates rather sharply.

3.2 Average Waiting Time in 1-Burst/D/1 Queue

In this subsection we discuss in more detail the average waiting time in 1-Burst/D/1 queue under low traffic load. For 1-Burst source, $P_I(t)$ can be interpreted as the probability that either the duration of the ON period or the duration of the OFF period exceed t:

$$\begin{aligned} \sum_{i=0}^{1} P_i(t) &= \Pr(S_{ON} \geq t) + \Pr(S_{OFF} \geq t) \\ &= 1 - \Pr(S_{ON} < t) + 1 - \Pr(S_{OFF} < t) \\ &= 2 - F_1(t) - F_2(t) \\ &= \left(\frac{\beta}{t}\right)^{\alpha} + e^{-\lambda t} \end{aligned} \tag{12}$$

Calculate the average value and we get:

$$\begin{aligned} E(\sum_{i=0}^{1} P_i(t)) &= E(\left(\frac{\beta}{t}\right)^{\alpha}) + E(e^{-\lambda t}) \\ &= \int_{\beta}^{+\infty} \left(\frac{\beta}{t}\right)^{\alpha} f_1(t)dt + \int_{0}^{+\infty} e^{-\lambda t} f_2(t)dt \\ &= \int_{\beta}^{+\infty} \alpha \cdot \beta^{2\alpha} t^{-2\alpha-1} dt + \int_{0}^{+\infty} \lambda e^{-2\lambda t} dt \\ &= 1/2 \cdot (1+1) \\ &= 1 \end{aligned} \tag{13}$$

From Eq.(8) and Eq.(13) we can conclude that the average waiting time of 1-Burst/D/1 queue is much similar to that of the corresponding M/D/1 queue under low traffic load. This indicate when network is not heavily loaded, traffic self-similar property has limited impact on network performance in terms of queuing delay, when can be predicted in traditional M/D/1 queuing models.

4. SIMULATION ANALYSIS

We build our simulation scenario in OPNET Modeler 8.0c. The node model in OPNET is illustrated in Fig.2. The process model *N_burst_src* generates self-similar traffic. The queue model *FCFS_Queue* is a queue model with FCFS service discipline and infinite buffer size. The service rate C_0 is a fixed value of 100,000 bytes/s. Packets in this scenario have a fixed size of 100 bytes. The N-Burst process has a shape parameter α of 1.4 and a location parameter β of 5.0. Parameter λ of OFF periods is fixed at 5.0.

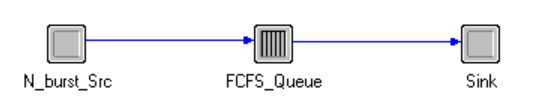


Fig.2. the simulated node model

4.1 Experiment 1 Average Waiting Time in N-Burst/D/1 Queue

In this experiment the number N of the sources is 10. Gradually increasing the sending rate κ of each source and run the simulation for 10 minutes, and the results compared with that of the M/D/1 queue are presented in Fig.3. It can be seen that under low traffic load both queue systems have low queuing delays. Queuing delays in M/D/1 queue are a little higher. While system utilization ratio ρ increases and approaches 1, queuing delays in N-Burst/D/1 systems are increasing at a much greater speed compared with that of the M/D/1 system. This indicates more sources enter the blow-up region and the queuing performance deteriorates sharply.

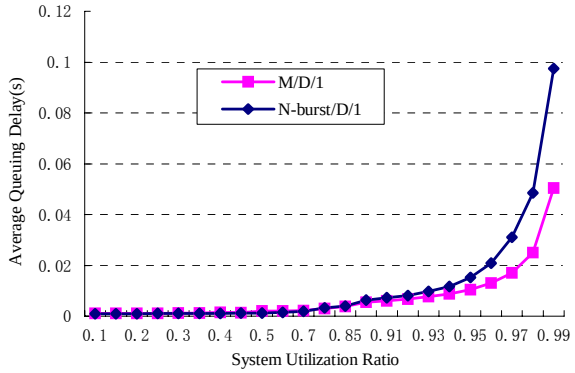


Fig.3. Average Queuing Delay versus System Utilization Ratio (N-Burst)

4.2 Experiment 2 Average Waiting Time in 1-Burst/D/1 Queue

Note that 1-Burst process has only one ON/OFF source, in this experiment the service rate is set to be C_0 =10,that is 10000 bytes/s. Follow a similar procedure in experiment 1 and the simulation results are presented in Fig.4.

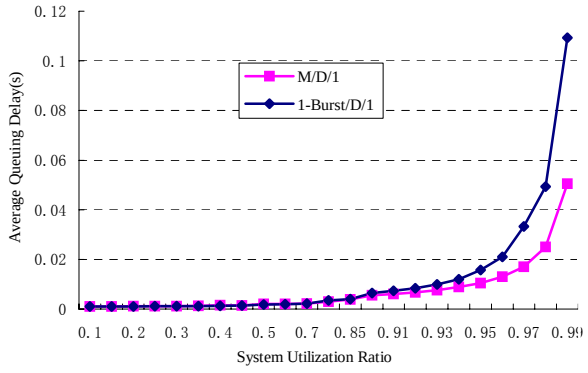


Fig.4. Average Queuing Delay versus System Utilization Ratio (1-Burst)

It can be seen from the graph that the average waiting time of 1-Burst/D/1 queue has a closer value to that of M/D/1 queue, compared with experiment 1. It can also been observed that the average waiting time of 1-Burst/D/1 queue increases more rapidly compared with that of N-Burst/D/1 queue, when system utilization ratio approaches 1.

5. CONCLUSIONS

This paper presents a new analytic queuing model with self-similar input traffic, namely the N-Burst/D/1 model. In-depth theoretical calculation and simulation results are presented. Our results show that under low traffic load the N-Burst/D/1 queuing system, especially the simple 1-Burst/D/1 queue, has close and smaller average queuing delays compared with that of the traditional M/D/1 queue with Poisson arrival process. When system utilization ratio approaches 1, we find that the queuing delays in N-Burst/D/1 far exceed that of the M/D/1 queue. Our results indicate the N-Burst/D/1 model is more accurate to reflect the self-similarity nature and queuing behavior of realistic traffic than traditional M/D/1 queue, and can be helpful to estimate network performance under dynamic network environments.

REFERENCES

[1] V.Paxson *et al*, "Wide area traffic: the failure of Poisson modeling," *IEEE/ACM Transaction on Networking*, 3(3), pp.226-244, 1995.

[2] A.Bhadra *et al*, "Simulation of An ATM Network using an ON-OFF model," In Proc. *IEEE Southeastcon2000*, Nashville, USA, 2000, pp.467-470.

[3] J.Sung-Ho *et al*, "Performance analysis of ATM queue under self-similar traffic," In *Proc. 5th IEEE International Conference on High Speed Networks and Multimedia Communications*, Jeju, Korea, 2002, pp. 213-217.

[4] J.Yu, *et al*, "Rate-Limited EAFRP:A New Improved Model for High-Speed Network Traffic," *IEEE Transaction on Signal Processing*, 53(2): 505-522, Feb 2005.

[5] H.Schewefel, *et al*, "Impact of aggregated, self-similar on/off traffic on delay in stationary queuing models," *Performance Evaluation*, 2001(43),pp.203-221.

[6] L. Lipsky, "Comparison of the Analytic N-Burst Model with Other Approximation to Telecommunication Traffic," In Proc. *IEEE International Symposium on Network Computing and Applications' 2001*, Boston, USA, 2001,pp.122-132.

[7] R. Nossenson *et al*, "The N-Burst/G/1 model with heavy tailed service-time distribution," In Proc. *IEEE MASCOTS' 2004*, Volendam, Netherlands, 2004, pp. 131-178.

[8] Y. Sheng, *Queuing Theory and its application in Computer Communications*, BUPT Press, Beijing, 1998.

Gongchao Su is a lecturer in College of Information Engineering, Shenzhen University. He got B.S and M.S degree in Communication Engineering in 2000 and 2003, from University of Electronic Science and Technology of China. His research interests are in wireless and high speed networking systems.

A Multicast Routing Algorithm of Multiple QoS for Mobile Ad Hoc Networks*

Niansheng Chen [1,2], Layuan Li [2], Zongwu Ke [2]
[1]Department of Computer Science, Hubei Normal University, Huangshi,Hubei 435002,China
[2]School of Computer Science, Wuhan University of Technology, Wuhan,Hubei 430063,China
Email: hschenns@163.com

ABSTRACT

Multicast routing is the process for establishing a tree which is rooted from the source node and contains all the multicast destinations. A multicast routing tree with multiple QoS constraints is the one in which the delay, delay jitter, packet loss and bandwidth should satisfy the pre-specified bounds. With the rapidly extensive applications of Ad Hoc networks, QoS multicast routing with multiple QoS constraints in Ad Hoc networks has become a very important research issue in the areas of networks and distributed systems. This paper discusses the multicast routing problem with multiple QoS constraints which may deal with the delay, delay jitter, bandwidth and cost metrics and describes a network model for researching the Ad Hoc networks QoS multicast routing problem. Then a multicast routing algorithm with multiple QoS constraints for Ad Hoc networks (MQRA) and the process of routing based on MQRA are presented. Moreover, the correctness of MQRA is proved and the complexity of the MQRA is analyzed. Simulation results show that the MQRA is an effective approach to multicast routing with multiple QoS constraints in Ad Hoc networks.

Keywords: Ad Hoc Networks, Multicast Routing, Qos Routing, Routing Protocol

1. INTRODUCTION

The mobile Ad Hoc networks (MANETs) refers to a temporal multi-hop autonomy system that is constituted by a group of mobile nodes with wireless send-receive equipment [1-13]. As an acentric, self-organized, fast-deployable, movable and multi-hop system, It can be wildly applied to many fields such as national defense, emergency and disaster, scientific investigation and exploration and so on. Therefore it has great prospects [1,4]. Every node in the Ad Hoc networks functions as both terminal and router. The limited bandwidth, unidirectional links which may appear at any time and the dynamic network topology caused by the nodes movement make it difficult to establish and maintain routing. So traditional fixed network routing technology cannot be adapted to the mobile Ad Hoc networks[1,4-12].

With the expansion of the fields in which mobile Ad Hoc network is used, the routing technology based on mobile Ad Hoc network has drawn many researchers' attention. And how to provide QoS in the Ad Hoc network and do researches based on QoS routing protocol of Ad Hoc networks has become an important topic in the field of network[1-4]. In recent years, many researchers have proposed some influential Ad Hoc network QoS routing protocols[5-12].Ref [5] presents MAODV which is applicable to Ad Hoc network. Although this protocol adopts following up the scent to deal with the change of multicast tree, it costs a lot and bases on "best effort service" principle. Ozaki and others [6] put forwards a bandwidth efficiency multicast routing protocol applicable to Ad Hoc network. But it cannot deal with the problem of multicast routing with multiple QoS constraints. Ref [7] brings forward a protocol based on constrains on bandwidth and energy to deal with the bandwidth wasting problem in Ad Hoc network. But this protocol doesn't support multicast. Lin [8] has designed the on-demand QoS routing protocol only adapting to unicast routing; Lee [9] and others have presented mobile Ad Hoc networks on-demand multicast routing protocol (ODMRP) based on grid, which has applied the conception of forwarding group and has successfully avoided the weakness of non-best-path and frequent reconstruction of a sharing-tree.The shortage is that the maintenance of current transmit group may cause redundant cost. On the basis of TBP[11] arithmetic, reference [10] makes definition of long-life links to avoid the dynamic change of network topology caused by the nodes movement and put forward a QoS routing protocol satisfying both the delay and the bandwidth (LBRM). But it doesn't offer any method or approach to support multicast. The contribution in Ref. [12] is QoS multicast routing protocol (QMRP) with constraints of bandwidth, delay, moving speed of node and the surplus electrical energy of node, however, it still exists imprecise in the definition of feasible path, besides only virtually considering the addable delay constraint.

Aiming at the characteristics of Ad Hoc network, this paper puts forward QoS multicast routing protocol (MQRA) with constraints of bandwidth, delay and delay jitter. This protocol defines feasible links among neighbor nodes through support of neighbor protocol [13].In routing, firstly an initial multicast tree is formed by unidirectional links from multicast source node to certain multicast destination node which satisfying multiple QoS constraints. Then other multicast destination nodes apply to join the multicast tree. Therefore a multicast tree satisfying multiple QoS constrains is swiftly and efficiently established.

The reminder of the paper is organized as follows. Section 2 discuss network model based on Ad Hoc networks and description the problem of QoS multicast routing with multiple QoS constraints. In Section 3, we present description and realization of MQRA. In Section 4, we analysis and prove the correlative characters of MQRA, present the time-complexity and the message-complexity of MQRA. Section 5 is Simulation and experiment. Finally, Section 8 concludes the paper.

2. DESCRIPTION of NETWORK MODEL and ROUTING PROBLRM

2.1 Network Model

A mobile Ad Hoc network can be manifested by a weighed digraph $G = (V, E)$, where V is the set of nodes in the network and E is the set of duplex links corresponding with nodes. Here $|V|$ is the number of nodes and $|E|$ is the number of links. If R_+ represents a set of positive data and R^+ represents a set of non-negative data, for any link $e \in E$, we can define the characteristic value of QoS : delay function $delay(e): E \to R_+$,

* Supported by the National Natural Science Foundation of China under Grant No.90304018, 60672137; The Grand Research Project of Hubei Province Department of Education in China under Grant No. D200622003

cost function $\cos t(e): E \to R_+$, bandwidth function $bandwidth(e): E \to R_+$, and delay jitter function $delay\_jitter(e): E \to R^+$. Meanwhile, for any node $n \in V$, we can also define the characteristic value of QoS: delay function $delay(n): V \to R_+$, cost function $\cos t(n): V \to R_+$, and delay jitter function $delay\_jitter(n): V \to R^+$. And in this paper we have formed following hypothesis: ①Because of the equality between nodes and links, we only consider QoS constrains of links in the following discussion. ②Every mobile node has an unique id and is supported by GPS in Ad Hoc networks. ③Each node has the same valid transmission range. If there are two nodes that are in the scope of each other's transmission range, we shall call them neighbor nodes, and there is a link between the two. ④By periodic broadcasting BEACON package neighbor nodes can identify itself and its neighbor node, and acquire the link circumstance between neighbor nodes [13].

2.2 The problem of QoS multicast routing with multiple QoS constraints

In Ad Hoc network $G=(V, E)$, If $s \in V$ is multicast source node, $M \subseteq \{V-\{s\}\}$ is multicast destination node sets, then there exists following relation in the multicast tree "$T(s,M)$" composed of "*s*" and "*M*":

(1) $delay(P_T(s,t)) = \sum_{e \in P_T(s,t)} delay(e)$.

(2) $\cos t(T(s,M)) = \sum_{e \in T(s,M)} \cos t(e)$.

(3) $bandwidth(P_T(s,t)) = \min\{bandwidth(e), e \in P_T(s,t)\}$.

(4) $delay\_jitter(P_T(s,t)) = \sum_{e \in P_T(s,t)} delay\_jitter(e)$.

$P_T(s,T)$ is the routing path between source node "*s*" and destination node "*t*" of multicast tree $T(s,M)$. So QoS multicast routing problem can be described like this: in the network $G=(V,E)$, $s \in V$ is multicast source node, $M \subseteq \{V-\{s\}\}$ is multicast destination node sets, delay function $delay(*) \in R_+$, delay jitter function $delay\_jitter(*) \in R^+$,cost function $\cos t(*) \in R_+$, and bandwidth function $bandwidth(*) \in R_+$, seeking a multicast tree $T(s,M)$ which suffice following conditions:

(1)delay constraint: $delay(P_T(s,t)) \le D_{\max}$

(2)bandwidth constraint: $bandwidth(P_T(s,t)) \ge B_{\min}$

(3)delay jitter constraint: $delay\_jitter(P_T(s,t)) \le J_{\max}$

(4)cost constraint: in the multicast tree sufficing above three conditions, $\cos t(T(s,M))$ is minimum.

$P_T(s,T)$ is the routing path between source node "*s*" and destination node "*t*" of $T(s,M)$. B_{min} is the bandwidth constraint, D_{max}、J_{max} and L_{max} are respectively delay constraint, delay jitter constraint and packet loss constraint.

3. DESCRIPTION and REALIZATION of MQRA

Definition 1: Supposing node *j* and node *i* are neighbor nodes, link $e(i,j) \in E$, *d(s,i)* and *dj(s,i)* respectively represent the sum of delay and delay jitter from multicast source node *s* to node *i* , if link *e* satisfies:

$(d(s,i)+delay(e)) \le D_{\max} \wedge (dj(s,i)+delay\_jitter(e)) \le J_{\max} \wedge bandwidth(e) \ge B_{\min}$

then link *e* is the feasible link satisfying Qos constrains.

Definition 2:The set of tree nodes Ω is the aggregate of all nodes in the multicast tree $T(s,M)$,and its initial value is {s}.

Definition 3: All the nodes in Ω memorize list LT(*node, upnode,dlt(node),djlt(node) clt(node)*), which mainly records information about some Qos constrains from certain node(*node*) to source node *s*, such as the value of delay(*dlt(node)*), the value of delay jitter (*djlt(node)*) and cost (*clt(node)*). Meanwhile, the parent-node(*upnode*) of that node is also recorded in LT.

In MQRA the establishment of multicast tree undergoes two phases: A initial multicast trees composed of unidirectional links is established firstly, then the source node *s* begins to routing request ,t_i($\forall t_i \in M$) is destination node of the routing, set up unicast link which satisfies Qos constrains. In the second phase, the other nodes in the set of multicast destination nodes *M* except t_i will apply to join the multicast tree. Finally the multicast tree $T(s,M)$ satisfying the requirements is formed.

3.1 Establishment of Initialization Multicast Tree

Before the multicast routing is established, a routing request message *Requ* with exclusive mark will be formed from source node *s* to certain multicast node $t_i (t_i \in M)$. *Requ* contains information about source nodes、destination nodes、Qos contains and links from source node to destination node. At the beginning of establishing routing, the source node *s* broadcasts *Requ* message to the neighbor nodes with feasible links.

When node *j* receive the *Requ* message from node *i* , node *j* will process like following:

Step 1: Supposing node *j* is not destination node t_i and has received *Requ* message, then it abandons the message and stops processing. Else it turns to Step 2.

Step 2: Node *i* becomes parent-node of node *j*, node *j* will mark that it has received *Requ* message and node *j* updates its link information list LT.

the mark of node *j* →*node;*

the mark of node *i* →*upnode*;

dlt(i)+delay(i,j) →*dlt(j);*

djlt(i)+delay_jitter(i,j) →*djlt(j);*

clt(i)+cost(i,j) →*clt(j);*

then node *j* joins Ω, $e(i,j)$ joins the link information of *Requ* message, and turn to Step 3.

Step 3: Supposing node *j* is not destination node t_i, then node *j* broadcasts *Requ* message to the neighbor nodes with feasible links,without mark of receiving *Requ* message ,and then stops processing. Else it turns to Step 4.

If node *j* can't find the neighbor node which satisfied all condition to transmit the message, it abandons the message, delete node *j* in Ω , repeal $e(i,j)$ in the link information of *Requ* message and node *j*'s mark of receiving *Requ* message. Then node *j* will mark relatively node *i* and node *i* chooses the feasible link to broadcast *Requ* message.

Step 4: If node *j* is the destination node t_i, the one in the request messages whose *clt(j)* value is minimum among the request message received within the prescribed time will become the result of request. Then ACK message is transmitted to the source node according to the link information recorded in *Requ* message and resource is reserved beforehand. While links information recorded in other messages will be saved as spare routing information. When the ACK message reaches the source node, unicast link

satisfying Qos constrains is established from the source node *s* to destination node $t_i(t_i \in M)$ and the initialization multicast tree is formed.

3.2 Dynamic Join of Destination Node

If multicast destination node $t_j(t_j \in \{M - \{t_i\}\})$ applies to join $T(s, M)$, firstly we should judge whether $t_j \in \Omega$ is true. When it is true, it means that node t_j is the member nodes of multicast tree. So the application task is finished; else, do as follows:

Node t_j produces request join message (*Rjoin*) with unique mark, whose data structure is $(s,t_j,D_{max},J_{max},B_{min}, Cd,path)$. "$s$" presents the source node, "t_j" is the destination node which applies to join the multicast tree, "D_{max}" "J_{max}" and "B_{min}" respectively represent initial value of delay, delay jitter and the minimal bandwidth value which satisfy this multicast Qos constrains. Cd=0 represents initial cost of link, $path$={ t_j } represents initial link. Node t_j broadcasts *Rjoin* message to neighbor nodes with feasible links satisfying Qos constrains.

When node *p* receives the *Rjoin* message from node *q* , it will do as follows:

Step 1: If node *p* has received *Rjoin* message, it abandons the message and stops processing. Else it turns to Step 2.

Step 2: Node *p* sets a mark of receiving *Rjoin* message and deal with the message as follows: the $e(q,p)$ joins the *path*, and $Cd = Cd + \cos t(q, p)$, $D_{\max} = D_{\max} - delay(q, p)$, $J_{\max} = J_{\max} - delay\_jitter(q, p)$, then it turns to Step 3.

Step 3: Judge whether $p \in \Omega$ is true. If it is not true, it means node *p* doesn't belong to the multicast tree, then turn to Step 4. Otherwise, judge whether $dlt(p) \le D_{\max} \wedge djlt(p) \le J_{\max}$ is tenable. If it is not tenable, cancel node *p*'s mark of receiving *Rjoin* message, delete the $e(q,p)$ in *path* and abandon the message and stop processing. Otherwise, node *p* sends request reversion message $Rack(s,t_j,path,Cd=Cd+clt(p))$ to destination node t_j and the processing ends.

Step 4: Node *p* broadcasts *Rjoin* message the node without the mark of receiving *Rjoin* message and with feasible links among its neighbor nodes, then the processing ends.

After sending the *Rjoin* message, the multicast destination node t_j will choose the one whose *clt(j)* value is minimum among the *Rack* message received within the prescribed time as the result of request. Then according to ACK message sent by *path* in *Rack* to the source node *s* the resource is reserved beforehand. When the ACK message from node t_j reaches the source node *s*, so node t_j successfully join the multicast tree $T(s, M)$.

The following specific example will illustrate the process of establishing a multicast tree. Supposing that Fig. 1 is the figure of Ad Hoc network topology temporarily established. The characteristics of links among the neighbor nodes are described by (*D,J,B,C*) which respectively represents delay, delay jitter, bandwidth and cost. Suppose certain multicast source node *s* is node 0, the set of multicast destination nodes is M={4, 9, 14, 19, 22}, and its QoS constraint values are: D_{max}=20, J_{max}=30, B_{min}=40.

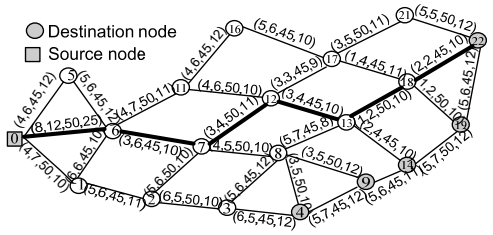


Fig.1. The network topology and initialization multicast tree

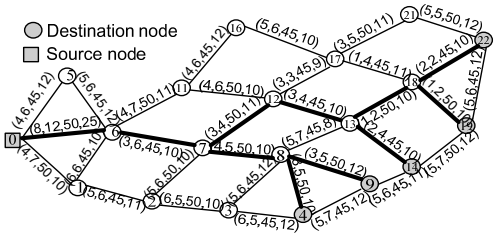


Fig.2. Multicast tree $T(s, M)$

First of all, the source node 0 broadcasts *Requ* message to nodes 1,5,6 establish initialization multicast tree whose destination node is node 22. When a certain node (e.g. node 7) receives the *Requ* message from node 6, it updates its link information list into *LT*(7,6,11,18,35), and let *e*(6,7) join the link information of *Requ*. Meanwhile,links *e*(7,2),*e*(7,8),*e*(7,12) are the feasible links satisfying current Qos constrains, so node 7 broadcasts *Requ* message to 2,8,12. Similarly after receiving *Requ* message node 8 finds that link *e*(8,13) is a feasible link, and then node 13 can receive *Requ* message sent by node 8 and deal with it. If node 13 receives *Requ* message from node 12, because of the existed receiving mark it abandons message without any processing. But after node 13 deals with the message sent by node 8, its link information list is *LT*(13,8,20,30,53), it doesn't have any neighbor nodes with feasible links. So it abandons the message, cancels the receiving mark and refuses to receive any *Requ* message from node 8.Therefore node 8 has to choose new feasible links to broadcast this message. In the same way node 18 cannot find feasible links after receiving *Requ* message from node 17, so it lets node 17 broadcasts *Requ* message again. And node 17 cannot succeed, so let node 12 broadcast messages again. Thus when node 13 receives *Requ* message sent by node 12 again, because of no receiving mark it can deal with the message and finally finds the feasible links like *e*(13,18). So a unicast link (0,6,7,12,13,18,22)(showed by the bold lines of Fig.1) satisfying Qos constrains is formed and an initialization multicast tree with Ω={0,6,7,12,13,18,22} is established.

In the second phase multicast destination nodes 4, 9, 14, 19 respectively apply to join the multicast tree. If node 4 applies, it broadcasts *Rjoin*(0, 4, 20, 30, 40, 0, {4}) to nodes 3,8,9. Receiving this *Rjoin* message node 8 which does not belong to Ω alters the message into *Rjoin*(0, 4, 17, 25, 40, 10, {4, 8}) and broadcasts this to nodes 3, 7, 9, 13. But nodes 3 and 9 have received the *Rjoin* message from node 4, so they abandon the message without any processing. Nodes 7 and 13 which belong to Ω deal with the *Rjoin* message sent by node 8. The result of node 13 is D_{max},=12,J_{max},=18, which does not satisfy $(dlt(13) = 17) \le D_{\max}$ and $(djlt(13) = 26) \le J_{\max}$. So node 13 abandons the message and cancels the mark of receiving message. However, the result of node 7 is D_{max},=13,J_{max},=20

which satisfies $(dlt(7)=11) \le D_{\max} \wedge (djlt(7)=18) \le J_{\max}$. So node 7 sends message $Rack(0, 4, \{4, 8, 7\}, 55)$ to node 4. When the *Rack* message is received by node 4, ACK message is sent to the source node 0 through link $\{4, 8, 7, 6, 0\}$. When the source node 0 receives ACK message, node 4 successfully join the multicast tree. In the same way nodes 9,14 and 19 can also join the multicast tree. Finally a multicast tree $T(s,M)$ satisfying Qos constrains is established. (showed by the bold lined in Fig.2)

In MQRA the multicast tree is established from the initialization multicast tree, so the nodes which doesn't belong to initialization multicast tree can dynamically join or quit the multicast tree without affecting the multicast tree. Meanwhile, each node of network only has to maintain the status message of its neighbor nodes regardless of the overall status message. Since the multicast tree $T(s,M)$ is established on the basis of feasible links, it can satisfy multiple Qos constrains.

4. ANALYSIS OF THE PERFORMANCE

The characters of MQRA protocol are proved in the following paragraphs.

Character 1 In the process of routing based-on MRQW, there are no loops in the paths that constitute the initialization multicast tree.

Prove: For $\forall d \in M$, source node *s* sends *Requ* message and node *d* is destination node. Supposing a path $p(s,d)$ from source node *s* to destination node *d* is formed in the process of routing, and parent-node of node *d* is node *k*. If there is loop in $p(s,d)$, then in the path $p(s,k)$ there must be some node receiving and transmitting *Requ* message twice without cancel the mark of receiving message. This is inconsistent with the requirement of establishing the initialization multicast tree. Thus, $p(s,d)$ is a path without loops.

Character 2 All the paths created in the process of routing based on MQRA will form a multicast tree $T(s,M)$ structure.

Prove: From character 1 we know the initialization multicast tree is a special tree structure whose only leaf node is multicast destination node. And other multicast destination nodes that apply to join the tree have their parent-nodes existing in the set Ω. So any node in the set Ω can only have one parent-node and all the leaf nodes in $T(s,M)$ are multicast destination nodes. Therefore $T(s,M)$ is a multicast tree structure.

Character 3 In a multicast tree $T(s,M)$, all paths from root-node (source node) to leaf-node (multicast destination node) satisfy multiple QoS constraints requirements.

Prove: In the process of forming the initialization multicast tree, each node only broadcasts *Requ* message to neighbor nodes with feasible links and the requirement of feasible links is $(d(s,i)+delay(e)) \le D_{\max} \wedge (dj(s,i)+delay\_jitter(e)) \le J_{\max} \wedge bandwidth(e) \ge B_{\min}$. No doubt, the paths obtained by the routing with above requirements satisfy delay, delay jitter and bandwidth constrains. When other nodes apply to join, the requirement they should meet is $dlt(p) \le D_{\max} \wedge djlt(p) \le J_{\max}$, p is the existing nodes in the set Ω, thus it satisfies multiple Qos constrains.

Character 4 In the process of routing based-on MRQW, under the worst circumstance the time-complexity is $O(k|V|)$ and the message-complexity is $O(3|m|)$. Here $|V|$ represents the number of Ad Hoc network nodes, *k* represents the number of their neighbor nodes, $|m|$ represents the number of multicast destination nodes.

Prove: The complexity of Qos multicast routing protocol can be analyzed on the basis of calculation complexity of multicast tree and the number of message needed. In the MQRA protocol if any node of network has *k* neighbor nodes, then this node broadcasts *Requ* message to *k* neighbor nodes at most. So for the nodes of network its the time-complexity is $O(k)$ and under the worst circumstance the time-complexity is $O(k|V|)$. In the MQRA protocol the multicast destination nodes which does not belong to the initial multicast tree need to transmit *Rjoin* message, *Rack* message and ACK message if they apply to join the multicast tree. So the message-complexity under the worst circumstance is $O(3|m|)$.

5. SIMULATION PROTOCOL

5.1 Simulation Environment

The simulation testing can be carried out in a scenario, whose node capacity is 100 and size is a 2200×1000*m* rectangle, where every node has a transmission range scope of 180*m*. If there are two nodes located at each other's transmission range scope, then there will be a link between them. The value of bandwidth between links get from a random data in the scope of (0~6) Mbps, the delay value and the delay jitter value of each link are evenly distributed between 5*ms* and 20*ms*. The value of link cost is distributed between 5 and 30. Each node selects its moving direction and speeds at random with the maximal speed is 30*m/s*, and every experiment scenario lasts 600*s*. All the simulation experiment results are the average value of many times of experiments.

5.2 Results of Simulation Testing and Performance Analysis

To evaluate the performance of MQRA algorithm, three algorithms are compared with MQRA; they are LBMR[10], QMRP[12] and Flooding[13]algorithm. The performance measures of interest are routing success ratio, multicast cost and multicast average delay.

When a multicast group has 20 nodes and the bandwidth constraint is 4Mbps, Fig.3 shows the routing success ratio of the different algorithms under different delay bound. In Fig.4, the routing success ratio of the different algorithms under different bandwidth constraint is presented, the delay bound is 150ms.

From Fig.3 and Fig.4, Flooding algorithm has the highest routing success ratio among these four algorithms under the condition of the different delay bound, and the routing success ratio of the MQRA algorithm is very near to that of the Flooding algorithm and higher than that of the LBMR and QMPR. When given the same delay bound, the routing success ratio of the MQRA algorithm is obviously higher than the other three algorithms. Thus the MQRA algorithm can be applicable in dynamic changed networks and be satisfied with the higher bandwidth constraint when only considering the routing success ratio. The results are reasonable, for the defined available link makes the MQRA algorithm not maintain the global state, and at the same time, the records in link information table also improve the routing success ratio.

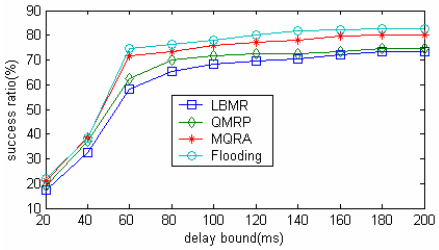


Fig.3. Success ratio under different delay bound

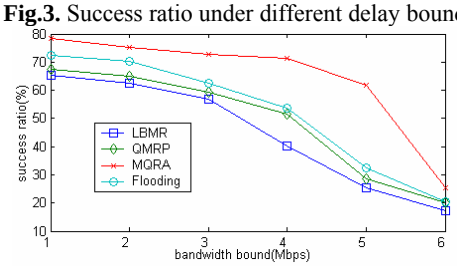


Fig.4. Success ratio under different bandwidth bound

Fig.5 presents the cost of multicast tree under different delay bound using these four algorithms. Fig.6 shows the average delay of multicast tree under the different size of network with the different algorithms. In Fig.5 and Fig.6, the size of multicast group is 20 nodes. From Fig.5 and Fig.6, the cost of multicast tree of the MQRA algorithm is the smallest among these four algorithms and with the size of networks increasing, the MQRA algorithm can also keep the smallest average delay among these four algorithms.

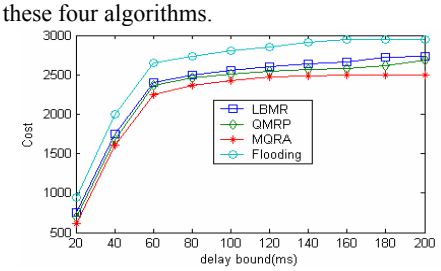


Fig.5. Cost of multicast tree under different delay bound

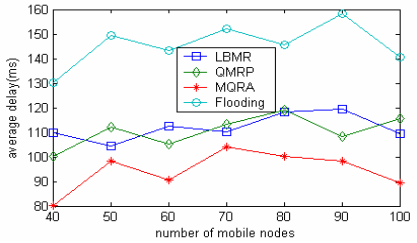


Fig.6. Average delay of multicast tree under different number of mobile nodes

It shows by simulation results that the MQRA algorithm has a better performance whether in the routing success ratio or in the cost and the average delay of multicast tree. The multicast tree generated by the MQRA algorithm can be satisfied with the Ad Hoc networks environment and provides a better QoS guarantee at the same time.

6. CONCLUSIONS

Aiming at the characteristics of Ad Hoc network, this paper puts forward MQRA multicast routing protocol satisfying multiple QoS constrains. Based on the definition of feasible links this protocol constructs multicast tree in two phases. And in the process of routing each node only needs to get the information about neighbor nodes but regardless of overall information. So the RSR increases and the complexity of carrying out this algorithm decreases. The simulation testing indicates that in the dynamic networks MQRA protocol can guarantee well the QoS constrains and perform very well.

REFERENCES

[1] Li La-Yuan,Li Chun-Lin. *Computer Networking*. 2nd ed. Beijing : National Defence Industry Press , 2004 (in Chinese).

[2] Chen Niansheng, Li Layuan,Dong Wushi. "A Multicast Routing Algorithm of Multiple QoS Based on Widest-Bandwidth." *Journal of Systems Engineering and Electronics* 2006,17(3), pp.642-647.

[3] Li La-Yuan,Li Chun-Lin. "A QoS_guaranteed multicast routing protocol." *Computer Communications*, 2004, 27(1), pp.59-69.

[4] Chen Niansheng, Li Layuan, Chen Chuanhui. "QoS Multicast Routing Algorithm based on Layered Structure." International Symposium on Distributed Computing and Applications to Business, Engineering and Science, *DCABES 2006, PROCEEDING*, pp.1135-1139.

[5] Royer E.M.,Perkins C.E.. "Multicast operation of the Ad Hoc on demand distance vector routing protocol." *ACM Mobicom*, 1999,(8) ,pp.207-218.

[6] Ozaki T.,Kim J.,Suda T. "Bandwidth efficient multicast routing protocol for Ad hoc networks".In:*Proceedings of IEEE ICCCN*, 1999, pp.10-17.

[7] Toh C K. "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks."*IEEE Communication Magzine,* Jun 2001, pp.138 -147.

[8] Lin C.-R.. "On demand QoS routing in multihop mobile networks." *In: Proceedings of IEEE INFOCOM* 2001,2001, pp.1735- 1744.

[9] Lee S.-J.,Su W.,Gerla M. "On demand multicast routing protocol in multihop wireless mobile networks." *ACM/ Kluwer Mobile Networks and Applications*,Jul 2002, (6), pp.441-453

[10] Shi Jian,Zou Ling. "A QoS based distributed multicast routing algorithm in Ad Hoc networks." *Journal of China Institute of Communications*,2003,24(6):60-68.

[11] Shigang Chen, Klara N, "Distributed quality-of-service routing in Ad-hoc networks." *IEEE Journal on Selected Areas in Communications*, 1999,17(8):1488-1505.

[12] SUN Bao-lin,LI La-yuan. "A QoS Based Multicast Routing Protocol in Ad Hoc Networks." *Chinese Journal of Computer,* 2004, 27(10), pp.1402-1407(in Chinese).

[13] Toh C-K. "Assiciatibity_based routing for ad hoc mobile networks." *Wireless Personal Communications* 1997, 4(2), pp.103-109.

Niansheng Chen is a Professor, Department of Computer Science, HuBei Normal University. Moreover, He is Ph.D candidate in Wuhan University of Technology. He got his bachelor's degree from HuBei Normal University in 1989 and master's degree from Wuhan University of Technology in 1999. His research interests are in Ad Hoc networks, QoS routing, and protocol engineering.

A Multicast Routing Protocol with Mobility Prediction in Ad Hoc Networks *

Peng Yang, Lei Chen
Maths and Computer Science Deparment of Chongqing University of Arts and Sciences
Chongqing, 402160, China
Email: llylab@21cn.com

ABSTRACT

Ad Hoc networks are collection of wireless mobile hosts forming a temporary and dynamic wireless networks with no fixed infrastructure or central administrator. In Ad Hoc networks, routes are mostly multihop and mobile hosts communicate via packet radios. Each host moves arbitrarily and thus routes are subject to frequent disconnections. By exploiting a mobile user's non-random traveling pattern, however, we can predict the future state of network topology and thus perform proactive rerouting process during the period of topology changes. In this paper we present an enhancement to MAODV protocol with mobility prediction. The results of simulation show that the scheme has better network performance.

Keywords: Ad Hoc Networks, MAODV, Mobility Prediction, Multicast, Simulator

1. INTRODUCTION

In typical application (such as disaster recovery, distributed collaborative computing and military communication) of Ad Hoc networks, nodes need to accomplish a task by group. Therefore, multicast routing protocol plays an important role in Ad Hoc networks. However, mobility presents a challenging issue for protocol design since the protocol must adapt to frequent changing network topologies and maintain the multicast tree efficiently. With the increasing speed, routes are subject to frequent disconnections. A reasonable multicast tree maintenance mechanism must be found to keep the connections. In this paper we present mobility prediction to enhance a typical multicast routing protocol-MAODV. Based on the prediction, routes are reconfigured before they disconnect.

The remainder of this paper is organized as follows. Section 2 presents the related work about mobility prediction. Section 3 describes an advanced multicast routing protocol (MAODV/MP) using the predicted information. In section 4, we present the simulation environment and evaluate the effectiveness of MAODV/MP. Concluding remarks are made in section 5.

2. RELATED WORK ABOUT MOBILITY PREDICTION

Mobility prediction focuses on distance for a time. In [1], it assumes that two nodes A and B are within the radio propagation range. Let V_A and V_B be the speeds, and θ be the moving directions of node A and B. Then the distance of the two nodes will be predicted base on the motion parameters. In [2, 3], T, the amount of time two mobile nodes will stay

connected is predicted with the similar approach and is given by:

$$T = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-bc)^2}}{a^2+c^2} \quad (1)$$

where

$a = v_A \cos\theta_A - v_B \cos\theta_B, b = x_A - x_B, c = v_A \sin\theta_A - v_B \sin\theta_B,$
$d = y_A - y_B$

All of the parameters of two neighbors are got by GPS [4]. And r is the transmission range. (x_A, y_A) is the coordinate of mobile node A and (x_B, y_B) is that of mobile node B.

Currently several wireless propagation model have been proposed and we can predict mobility of node based on received signal strength [5]. In [6], the link expire time t between neighbor nodes is given by:

$$t = \frac{-b+\sqrt{b^2-4ac}}{2a} \quad (2)$$

where

$a = t_2\sqrt{P_1P_s}\beta, b = \sqrt{P_s}((\sqrt{P_1}-\sqrt{P_2})-t_2^2\sqrt{P_2}\beta),$
$c = t_2\sqrt{P_2P_s}-t_2\sqrt{P_1P_2}$
$\beta = \frac{\sqrt{P_1P_2}t_2+\sqrt{P_2P_3}t_3-\sqrt{P_1P_3}t_3-\sqrt{P_2P_3}t_2}{(t_2t_3^2-t_3t_2^2)\sqrt{P_2P_3}}$

P_1, P_2 and P_3 are three received packets' signal power strength at time t_1, t_2 and t_3 respectively. P_S is the threshold of receiving signal power. It is a precise method to predict expire time.

3. MAODV WITH MOBILITY PREDICTION PROTOCOL (MAODV/MP)

In this section, we propose MAODV/MP which utilizes the mobility prediction mechanism to maintain multicast tree prior to route disconnection based on MAODV protocol. In our approach, we assume a free space propagation mode, where the received signal strength solely depends on its distance to the transmitter. While nodes receive multicast packets, they record the time and the received signal strength. Then the link expire time between the two nodes will be calculated by Eq. (2). If the value less than that contained in data packets received, the link will be marked *soon to be broken*. The downstream node of the neighbors triggers rerouting process. The maintenance of multicast tree includes state updating and multicast tree branch rebuilding.

3.1 State Updating

It is triggered when a node predicted the link will be broken based on the packets received from its neighbor. The state soon to be broken will be inserted into routing table entry of the upstream node only if one of neighbor nodes discovery the

* This work was supported by the science and technology research project of chongqing municipal education commission under grant KJ071203 and the key research project of chongqing university of arts and sciences under grant Z2006SJ30

latent disconnection. Thus, in spite of the direction of flow

between neighbor nodes, the upstream node always suppose the link will be broken and the rerouting process will be initiated. In original MAODV [7], however, maintenance of multicast tree is called by downstream node after the link was broken. Data packets will dropped because of route disconnection before a new route is found. In MAODV/MP, on the contrary, data packets transmission will go on if link is not really broken.

3.2 Multicast Tree Branch Rebuilding

It is triggered by downstream node when it predicts the link will be broken. It begins to send routing request message. If the node do not receive reply message within a definite time, it will not increase the expire time of RREQ to broadcast RREQ message again until the time exceed the predefined one.

Downstream node sends RREQ-J extension packet. The packet includes information about hops between downstream node and group leader and differs with that in process of multicast tree building. In this way, downstream of a node will not reply the RREQ-J packet based on the information. The group membership which receive RREQ-J extension packet need examine the hops to group leader. When the hops are less than those in RREQ-J extension packet, the group membership can reply the packet. Otherwise, relay nodes will broadcast RREQ-J extension packet. The node which receives RREQ-J packet will check the state of the reverse link to its neighbor. If the state marks soon to be broken, it must discard the RREQ-J extension packet.

Once RREP-J packet is unicast to source node along the reverse route which RREQ-J packet transmit, a new multicast branch is built. While RREP-J packet is sent, relay nodes will also check the state of link. If the state marks soon to be broken, it also discard RREP-J packet. When the source node receives RREP-J packet, it will chose a route which the hops to group leader is the least and the sequence number is the largest. Then it begins to send MACT-J packet to active the new route and send MACT-U packet to its downstream node for updating the hops to group header. Upstream of source node changes in the new multicast tree branch, while the former upstream node still can send packet to source node until the old link is really broken.

Figure 1 shows an example of multicast tree maintenance process. When node B receives a multicast packet, it calculates the expire time of link AB following equation 2 based on the moment of received packet at last three times and the power of receiving signal. If the link is to be broken, node B will broadcast RREQ-J extension packet to build a new multicast tree branch. Once node B receives RREP-J packet, it will chose a route which the hops to group leader is the least and the sequence number is the largest. Then it begins to send MACT-J packet to active the new route. So before link AB broken, a new multicast tree branch (node B is the source node) will be probably built so as to enhance packet deliver ratio of the network.

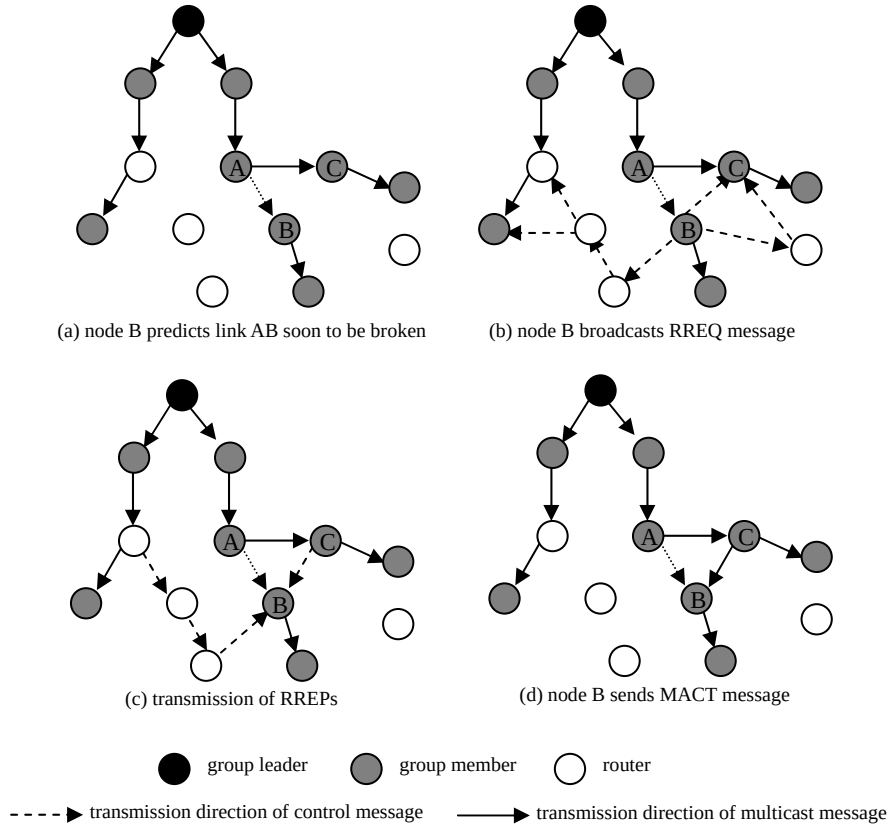


Fig. 1. Multicast tree maintenance in MAODV/MP.

4. SIMULATION EXPERIMENT

We implemented the simulator within OPNET Modeler. The IEEE 802.11 Distributed Coordination Function [8] was used as the medium access control protocol. Our simulation modeled a network of 50 mobile nodes placed randomly within an 800 meter × 600 meter area. Each node has a radio propagation range of 250 meters and channel capacity was 2 Mb/s. The size of data payload was 512 bytes. The

performance evaluation parameters include end-to-end delay and packet delivery ratio.

Figure 2 shows the end-to-end delay as function of group scale. We can see that as group member increase, the routing effectiveness of two schemes both degrade. When the group member exceeds 30, the delay of both protocols rises rapidly. Multicast tree growing leads packets transit more hops. Moreover, a node may synchronously have several downstream nodes in growing multicast tree. Queuing of packet and congestion in the node will probably often happen, contributing more delay.

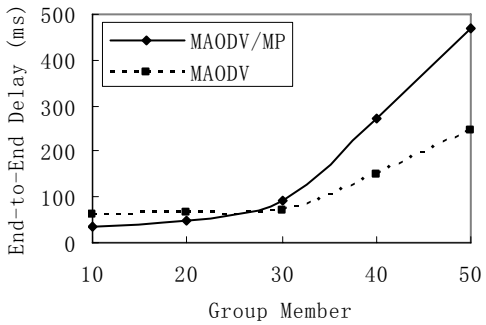


Fig. 2. End-to-end delay as function of group scale.

Figure 3 shows the packet delivery ratio as a function of group scale. As group members increase, the performance of two schemes both degrades. When the group member is less than 20, the packet delivery ratio of MAODV/MP maintains above 0.9. When the group member exceeds 30, however, the packet delivery ratio drops sharply. For most nodes are group members and more multicast tree branches form at this time, mobility of nodes will increase difficulties of rerouting and route overload of control messages rise gradually.

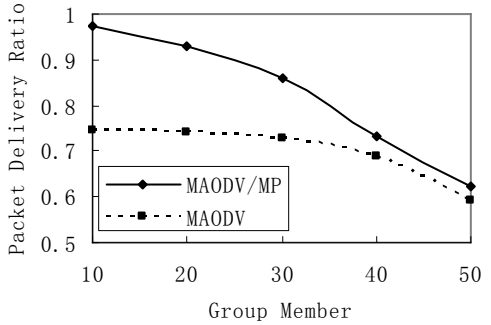


Fig. 3. Packet delivery ratio as a function of group scale.

Figure 4 shows the end-to-end delay as function of mobility speed. As nodes move faster, the delay of two schemes increases slowly and the increment of MAODV/MP grows faster compared with MAODV. For link state prediction scheme brings more process of multicast routing maintenance and makes multicast tree grow. And then the average hops packets pass through increase so that the delay rises.

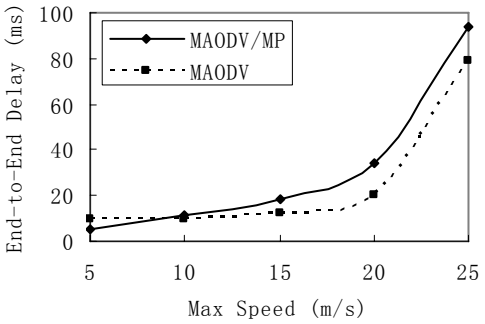


Fig. 4. End-to-end delay as function of mobility speed.

Figure 5 shows the packet delivery ratio as a function of mobility speed. As speed increases, the routing effectiveness of both protocols begins to degrade because the probability of link to be broken adds and division and repair happen continually. The average packet delivery ratio of MAODV, however, degrades remarkably compared with MAODV/MP. The ratio of MAODV/MP maintains above 0.9 while MAODV about 0.6. We can see that in the high speed scenario the MAODV/MP protocol has obvious advantage.

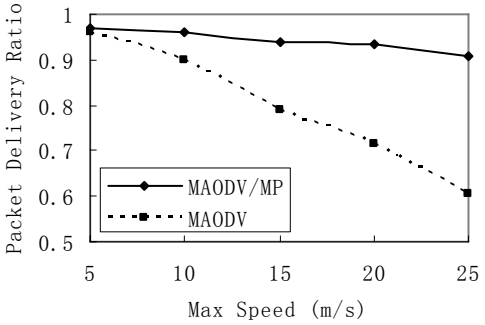


Fig. 5. Packet delivery ratio as a function of mobility speed.

5. CONCLUSIONS

In this paper we applied mobility prediction mechanism to Ad Hoc network multicast routing protocol. In the advanced protocol MAODV/MP, nodes can predict the expire time of link based on the received time and signal of packet from their neighbors. The protocol can perform proactive rerouting prior to route broken. Simulation results indicate that with mobility prediction enhancements, more data packets were delivered to destination. Especially in the high mobility scene, its advantage is obviously.

REFERENCES

[1] Lee S J, Su W, "Ad hoc wireless multicast with mobility prediction", Proc IEEE ICCCN, Boston, 1999, pp.234~256.

[2] Deng Shuguang, "A Unicast Routing Rrotocol Based on Mobility Prediction in Mobile ad Hoc Wireless Networks", *Journal of Computer Engineering and Applications,* Vol.34, No.14, 2002, pp.152~156.

[3] Su,W., Gerla,M, "IPV6 Flow Handoff in Ad-Hoc Wireless Networks Using Mobility Prediction", *Proceedings of IEEE Global Communications Conference,* Rio de Janeiro, Brazil, December 1999, pp.271~275.

[4] E.D.Kaplan, "Understanding the GPS. Principles and Applications", Artech house, 1996, pp35~52.

[5] Rappaport, T.S., "Wireless Communications. Principles and Practice (2nd Edition)", Prentice Hall, 2002, pp.79~94.
[6] Qin, L., "Pro-active Route Maintenance in DSR", M.Sc. Thesis, School of Computer Science, Carleton University, August 2001, pp.19~56.
[7] E.M.Royer, C.E.Perkins, "Multicast Operation of the Ad Hoc On-Demand Distance Vector Routing Protocol", *Proceedings of ACM/IEEE MOBICOM'* 99, Seattle, WA, Aug 1999, pp.207~218.
[8] Hang Su, Peiliang Qiu, "IEEE 802.11 distributed coordination function : performance analysis and protocol enhancement", *Advanced Information Networking and Applications*, 2004, pp.335~338.

Peng Yang is a lector of Maths and Computer Science Deparment of Chongqing University of Arts and Sciences. He graduated from the School of Computer Science and Technology of Wuhan University of Technology in 2006 and acquired the master degree. He has taken part in projects of two National Natural Science Foundation of China and published two Journal papers. His research interests are in network applications and routing protocols.

Lei Chen is a lector of Maths and Computer Science Deparment of Chongqing University of Arts and Sciences. She graduated from the School of Computer Science and Technology of Chongqing University in 2006 and acquired the master degree. She has published three Journal papers. Her research interests are in network applications and grid computing.

Research on High Performance Network Congestion Control*

Zhongyu Li[1], Haibo Wu[1], Hong Wen[1], Huifu Zhang[1,2]
[1]College of Information and Electrical Engineering，Hunan University of Science and Technology
Xiangtan, Hunan, 411201, China
[2]Wuhan University of Technology Wuhan, Hubei, 430070, China
Email:lizhongyu5336@126.com

ABSTRACT

Early research on network congestion control focused on improving TCP congestion control, which has obtained some achievements. But with the wide use of optical fiber, high performance router and a large amount of application software, the network's performance has been rapidly improved. Under such circumstances, the conventional TCP congestion control mechanism and IP drop tail mechanism cannot meet the requirements of congestion control for today's high performance network. This paper proposes a congestion control architecture for high performance network, which can improve the conventional congestion control architecture at the TCP layer and the IP layer. It solves network congestion problems caused by UDP strings and TCP-unfriendly strings possessing overabundant bandwidth; meanwhile, it can also help solve such problems as global synchronization, lock out and full queue to a certain extent and thus, improving the link utilization.

Keywords: High Performance Network, Congestion Control, Global Synchronization, Lock Out, Full Queue

1. HIGH PERFORMANCE NETWORK CONGESTION CONTROL

The conventional congestion control consists of the TCP congestion control mechanism and the drop tail queue control of the router. The TCP detects the network capacity by slow start and it will promptly lower the speed of message delivering to control the congestion as soon as it receives the signal of congestion message. The router won't reject the packets until the queue in the buffer is fully loaded. Then the TCP and the router form a simple closed-loop control to ensure the stability of the network.

With the development of the network technology, the conventional network congestion control architecture can no longer meet the requirements of today's high performance network congestion control. What is high performance network? First of all, it refers to the rapid increase of the network backbone bandwidth and speed of network. The network hardware technology has been improved greatly and the typical backbone bandwidth has been over Gigabit because of the wide use of optical fiber. The high performance router increases the speed of packet forwarding, which has solved the bottleneck of network to a certain degree. Secondly it refers to the continuous emergence of various network applications on the basis of the greatly improved performance of network hardware. The current network applications include the enormous real-time flow caused by audio- and video-frequency, IP telephone call, network games, etc., which need the guarantee of QoS. And the rapid expansion of the network scale has brought about much more file flow. Therefore, the high performance network need better congestion control.

We hereby propose a congestion control architecture based on the high performance network, which is co-controlled by the source terminal (TCP layer) and router (IP layer). This can be illustrated as follows:

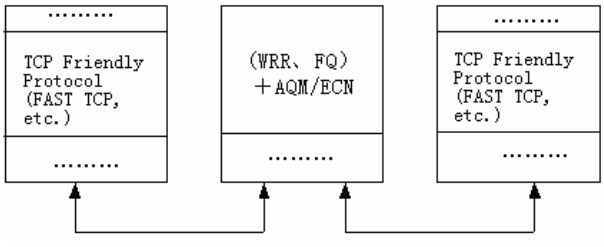


Fig.1. The High Performance Network Congestion Control architecture

Our studies of this system:

(1) Use the TCP friendly protocol as much as possible at the source terminal. Some so-called fast TCPs are actually against the stipulation purposely that response should be made to the network congestion under TCP, at the same time, there is a great increase of the application of UDP as a transmission layer protocol on Internet. UDP, as an open-loop protocol, has no congestion control by itself. When the congestion occurs, the TCP which have no congestion control mechanism and UDP will make no response to it; this will bring about serious unfairness and even make the network break down because of the congestion. So we prefer the application of the FAST TCP.

(2) As to the queue scheduling, we suggest the use of FQ (Fair Queue), Round Robin, or WRR (Weighted Round Robin), etc. The queue scheduling can better solve the problem of over-possessing the bandwidth by the UDP flow and other non-TCP friendly flow, and avoid the network congestion to some extent.

(3) As to the queue control mechanism of the router, we suggest the AQM/ECN mode be used. The conventional router queue control adopts the PQM/Drop mode, which easily brings about such problems as global synchronization, lock out, full queue and the low link utilization. To solve the problems, IEFT suggests the application of AQM/ECN mode in the router. ECN notifies the TCP source terminal of congestion through the setting at the IP packet header instead of Drop. It can also reduce the unnecessary rejection of messages at the earlier stage of congestion so as to increase the link utilization.

We'll focus on the effect of the queue scheduling and ECN on the network congestion control in this system.

*National Natural Science Foundation of China(NO.60673169)
A Project Supported by Scientific Research Fund of Hunan Provincial Education Department(NO.05C184)

2. USE QUEUE SCHEDULING MECHANISMS TO SOLVE THE NETWORK CONGESTION CAUSED BY UDP FLOW

2.1 Main Queue Scheduling Mechanisms

The queue scheduling aims to schedule the messages in different queues in the router to meet the requirement of different flows to QoS on the Net. The classfier categorizes different groups and sends each group to the corresponding queue. Then the scheduler decides which group will be selected and sent to the link to guarantee the quality of service required by the flow. At present, the widely used are the Fair Queue algorithm and the Round Robin algorithm.

(1) The Fair Queue Algorithm
Nagel proposed the Fair Queue algorithm in 1987. It maintains an independent queue for each flow passing by the router so that noninterference exists between queues. When the output link is vacant, the router will scan round every queue to select a packet and send it out; when the network is congested, the rejected are always the packets in the longest queue.
By analyzing Nagel's algorithm, we can see the following problem: if the packet of flow is very large, the bandwidth occupied by it will be more than that of the flow using the smaller one. To correct the defect, Demers and others designed an improved scheme in 1990, the main purpose of which is to scan round a byte instead of a packet each time.

(2) The Round Robin Algorithm and the WRR (Weighted Round Robin) Algorithm
The core of the Round Robin algorithm is that the scheduler serves each flow in turn. If the scale of each packet is the same, the Round Robin algorithm can guarantee the fairness of the bandwidth among flows. Otherwise, it's hard to ensure the fairness. So it means the Round Robin algorithm also lays stress on the flow of large packet in allotting the bandwidth.

WRR is used to meet the requirements of flows of different priorities to the bandwidth. According to the Round Robin algorithm, it assigns tasks to each flow on the basis of the value of weight. The flows with higher weight value will process more tasks than the lower one, and the flows with same value will process the same share of tasks. That is, the higher values of weight are allotted to those flows demanding high bandwidth.

2.2 Use WRR Mechanisms to Solve the Congestion Caused by UDP Flow[4]

Sally Floyd and Kevin Fall [4] suggested distinguishing the TCP flow from the open-loop flow which has no response to the indication of congestion in the router, using the queue scheduling to make the allotment of bandwidth fairer and reducing the probability of congestion. By using the topological diagram in Fig. 2, conduct the simulation experiment on the platform of NS (Network Simulator).

The experiment verifies these: if the conventional FCFS mechanism is adopted in the network of mixed TCP and UDP flow, it will make the bandwidth allotment unfair and bring about the congestion easily; but using the WRR algorithm in the same network can efficiently avoid the unfair allotment of bandwidth and network congestion.

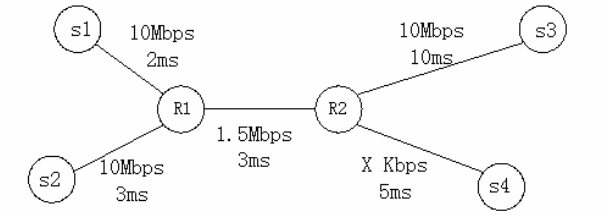


Fig.2. The Network Topological Diagram of The Queue Scheduling Mechanism Experiment

In Fig. 2, there are 4 nodes — S1～S4, two router — R1 and R2; the bandwidth and transmission delay time of each link are marked beside the corresponding link. Flows in the Fig. include:

(1) three TCP links from S1 to S3, each with the transmission of data all the time.
(2) one UDP flow of constant speed from S2 to S4.

The highest speed of UDP flow is 2Mbps. In the experiment, the thick continuous line stands for the total good output, the thin one for the good output of the TCP flow, the dotted line for the good output of the UDP, the broken line for the arrival rate of the UDP flow in the router.

Sally Floyd and Kevin Fall [4] discussed the congestion collapse caused by the undelivered packets. That happens because the bandwidth is wasted by the packets refused before reaching the host. It is mainly caused by that applications which do not use the end-to-end congestion control mechanism such as UDP. Some applications even increase the delivering rate when the refusing rate of packets increase, which makes the situation worse.

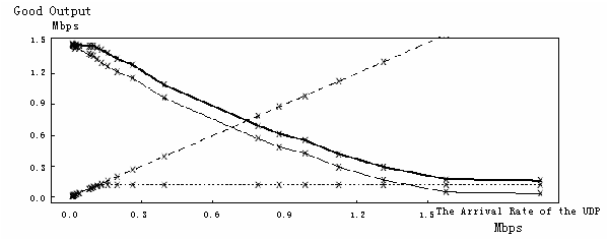


Fig.3. Congestion Collapse Caused by UDP

Such congestion collapses will not take place when the bandwidth of congestion link isn't high and the bandwidth between the receiving node and the router is very large. But if the bandwidth between them is smaller than that of the congestion link, such collapses will happen more frequently..

Fig. 3[4] is based on the simulation experiment adopting the topological diagram in Fig. 2, in which the bandwidth of the link from R2 to S4 is 128 kbps and adopts the FCFS scheduling algorithm. In Fig. 3, under the FCFS scheduling algorithm, when the arrival rate of UDP increases linearly, the good output of UDP increases linearly at first and then keeps at 128k; but the good output of TCP decreases dramatically with the increase of the arrival rate of UDP. When the arrival rate of UDP is up to near 1.5M, the good output of TCP decreases to nearly 0 and the comprehensive good output decreases to about 128k, which we call congestion collapse.

The conclusion in Fig. 3 shows that most UDP packets are refused by the router R2 because the bandwidth of link from R2 to S4 is much smaller than that of link from R1 to R2. The bandwidth over 128kbps in R1 to R2 occupied by UDP packets are wasted, and the congestion collapse caused by the undelivered packets makes the good output of the network

near to zero. To the UDP flows, it brings no benefit because the receiving end of the UDP flows doesn't use those bandwidths. But to the TCP flows, the collapse is a disaster because the bandwidths abandoned by them are not efficiently utilized and the good output of them is near to zero. So this kind of congestion collapse is one of the biggest problems unsolved on Internet, which need people's more attention with the increasing of application based on UDP on Internet.

The topological diagram and the network scheme in Fig. 4[4] are nearly the same as those in Fig. 3 except that it adopts the WRR scheduling mechanism instead of FCFS. The bandwidth in R1 to R2 occupied by the UDP flow is confined to about 25% and the good output of the entire network is a little lower. WRR plays an important role in preventing the congestion collapse.

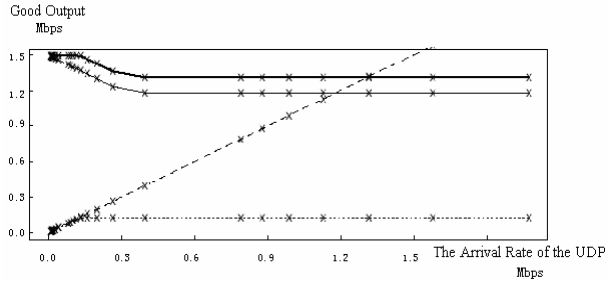


Fig.4. Use WRR to solve the Congestion Caused by UDP

The above experiment shows that the application of queue scheduling algorithm as WRR and WFQ can effectively control the network congestion and make the allotment of bandwidth fairer. But the WRR scheduling algorithm cannot solve all the problems. When the UDP flows in Fig. 4 increase to 3 and the TCP flow falls to 1, the comprehensive good output can only reach to about 35% even by using the WRR scheduling Mechanism. Sally Floyd and Kevin Fall held that the congestion collapse are caused by the undelivered packets results from the UDP's lack of end-to–end congestion control but not the scheduling algorithms used by the routers. They also pointed out that the end-to–end congestion control must be used in grouping network to prevent the flow from keeping sending packets when most of the packets in the flow are refused.

3. ADVANTAGES OF USING ECN MECHANISM

3.1 ECN Mechanism[5, 6]

AQM begins to refuse the packets when the average queue length exceeds a certain threshold value; that is, it refuses the packets when the queue is still not filled. By this, AQM can effectively control the average queue length, but it also wastes the network resource and is not an ideal mechanism to the multimedia application. Therefore, AQM can use other methods instead of refusing packets as means of notifying congestion, in which ECN(Explicite Congestion Notification) is one of the congestion notifications suggested by IETF.

ECN needs to set up a 2-bit ECN domain at the IP message header: one is ECT (ECN-Capable Transport) bit, which is set up by the TCP source terminal to show that the transport protocol supports ECN; the other is CE (Congestion Experienced) bit, which is set up by the router to show whether the congestion takes place or not.

When TCP use three-way handshake mechanism to sets up the connection, the source sets up an ECN—Echo bit to support ECN at the header. The receiving end sends back an acknowledgement to this packet and sets up an ECN—Echo bit. Then the source sends a acknowledgement to the receiving end, and a TCP link supporting ECN is set up. After that, the source sets ECT bit as 1 at all the headers. When the packet is sent to the router, the router will check the ECT bit of IP packet before it decides whether to refuse the message or not. If the ECT bit has been set, the CE bit in the IP message segment will be set as 1 to show the congestion, or the packet will be refused. After receiving the packet with the CE bit set as 1, the receiving end sets the ECN—Echo bit of the ACK message segment to be sent. Having received the set ACK of the ECN—Echo, the source end halves the congestion windows, sets CWR (Congestion Window Reduced) in the first IP packet to be sent, and not responds to the following congestion notifications. Finally, the receiving end stops setting the ECN—Echo on ACK packet after it has received the packet which has been set CWR bit.

3.2 The Comparison Between the Performances of ECN and Drop[7]

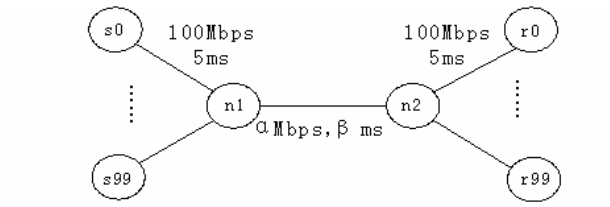


Fig.5. The Network Topological Diagram of the Comparison Between the Performances of ECN and Drop

Simulate the network in Fig. 5, and set α=20，β=30. The simulation comparison is made under the mark modes of ECN and Drop by adopting 100, 200 and 300 flows in the experiment separately, the result of which is shown in Fig. 6. From the Fig., we can see: the average queue lengths of TCP_ECN and TCP_Drop are almost the same when the indication probability of congestion is lower; with the increasing indication probability of congestion, the descending rate of the average queue length of the TCP_ECN flow is apparently lower and more stable than that of the TCP_Drop flow. We can draw the following conclusions from Fig. 6:

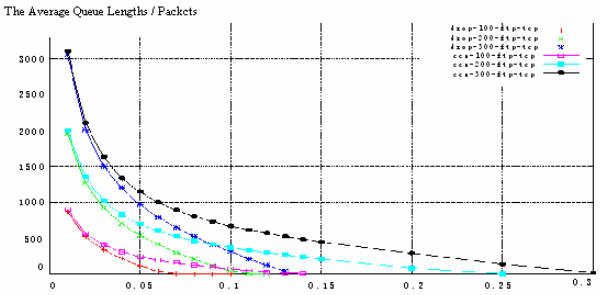


Fig.6. The Comparison Between the Performances of ECN and Drop

(1) If we hope that the router can maintain a reasonable average queue length target (such as 500 messages in Fig. 6) when the load increases linearly, then the stable rate of Drop and ECN will increase exponentially. The difference is that ECN increases more rapidly than the Drop does. From the queue curves of ECN, we can see that the average queue length inclines to 0 comparably smoothly when the mark

probability approaches to 1, which means the ECN mode can have a mark probability to keep the queue length at a lower level even in the case of heavy load.

(2) When the rate of mark/Drop increases, the queue curves of ECN mode descend more smoothly and stably than those of Drop mode. To the AQM algorithm, this means the average queue length of the router will be more stable under the ECN mode.

(3) If RED and ECN are combined and the congestion is detected before the queue is filled, the congestion notified by ECN mode can avoid unnecessary packet drop and be more efficient to a short or delay sensitive TCP link. Meanwhile, ECN avoids unnecessary time-out retransmission of TCP.

4. CONCLUSIONS

By summarizing the existing congestion control mechanism, this paper proposes a congestion control architecture based on the current high performance network. The validity of the network congestion control architecture has been verified by analyzing the existing researches. As to the other two important problems—the congestion control of TCP and AQM and its improvement, we will conduct further research on them in the future.

REFERENCES

[1] Cheng, Jin, David X. Wei, and Steven H. Low. "FAST TCP: Motivation, Architecture, Algorithms, Performance." In the *Proceedings of IEEE Infocom*, Hong Kong, March, 2004.

[2] Chung, Jae, and Mark Claypool, "Analysis of Active Queue Management." *In proceedings of the 2nd IEEE International Symposium on Network Computing and Applications*(NCA), Cambridge, Massachusetts, USA, Apr 2003.

[3] Demers A. Keshav S. and Shenker S. "Analysis and Simulation of a Fair Queueing Algorithm" *Internetwork: Research and Experience*, Sept. 1990,vol 1 3~26

[4] Floyd, S. "TCP and Explicit Congestion Notification." *ACM Computer Communication Review*, 1994, 24(5), pp.10~23.

[5] Floyd, Sally, and Kevin Fall "Promoting the Use of End-to-End Congestion Control in the Internet." *IEEE/ACM Transactions on Networking* May 3,1999

[6] Nagle J. *On Packet Switches with Infinite Storage.* RFC 970,1985.

[7] Ramakrishnan, K.K. and Jain R. "A Binary Feedback Scheme for Congestion Avoidance in Computer Networks." *ACM Computer Communication Review*, 1990, 30(1), pp.23~36.

Zhongyu Li is currently a lecturer in Hunan University of Science and Technology. He received his BS degree of industry automatic from Xiangtan mining Institute in 1993 and the MS degree of computer network from Wuhan University of Technology in 2007 respectively. His research interests include computer network and communications.

A Least-cost Multicast Tree Generation Algorithm with Delay Constraint Based on Application-layer

Kunhua Zhu[1], Xianfang Wang[1,2]
[1.] College of Information and Engineering, Henan Institute of Science and Technology
Xinxiang, Henan 453003, P.R.China;
[2.] School of Information & Control Engineering, Southern Yangtze University, Wuxi 214122, China
Email: zwkh100@163.com

ABSTRACT

Multimedia real-time transmission, which are both delay and transmission cost sensitive, is an important aspect of application-layer multicast technology. Careful study of constructing a multicast tree with low delay and cost is a pre-condition for completing the multicast task with high quality and low cost in the internet. Multicast routing problem with delay constraints is the equal of finding the solution to the delay-constrained least-cost NP-hard problem.[1] Lagrange relaxation algorithm can deal with combinatorial optimization problem preferably[9]. It integrate delay and cost as a consideration by Lagrange relaxation factor and change the specific gravity of delay and cost in the process of finding solution to the multicast tree by adjusting the relaxation factor , thereby obtaining the satisfactory solution. Lagrange relaxation was first introduced into the paper, and according to this, we proposed an algorithm to find solutions to least-cost multicast tree under a given delay bound for the application-layer multicast. For this algorithm can combine the different factors (cost and delay) as a unified factor and obtain a multicast tree which is near-optimal solution. The simulation experimental results demonstrate the effectiveness of the algorithm
.

Keywords: Application-Layer Multicast, Lagrange Relaxation, Delay Constraint, Least-Cost Multicast Spanning Tree

1. INTRODUCTION

Some researchers begin to reflect on the problem of IP multicast architecture itself facing the plight of IP multicast service in the Internet .They proposed the new idea to realize the complicated multicast function in the end system. It regards multicast as an overlay service and realize the service for the application layer .So the end system multicast is known as application-layer multicast. The nodes of application-layer network are multicast member hosts. The functions of Data routing, copy and delivery are all completed by member hosts. Member hosts are established on an overlay network and the hosts establish and defend the overlay network based on self-organization algorithm [2-7]. The data of IP multicast realize their copy and delivery along the physical link, but all these functions can be realized in the hosts for the application-layer multicast .The multicast data delivery along the multicast tree contrasted on the overlay network (Logical link) multi-hop logical link can be pass the same physical link. Comparing with IP multicast, application-layer multicast has many advantages, such as it can dispose at any time and expand easily. Of course, it has its own disadvantages also for example, its efficiency doesn't as good as IP multicast; its reliability can be effected easily by the stability of the end system. Furthermore, it's very important to know how to generate a multicast tree quickly and effectively in application-layer multicast .This paper proposed a new delay-constrained least-cost multicast tree generation algorithm based on Lagrange relaxation. It combines the two independent factors (cost and delay) by Lagrange relaxation and obtains the polymerization cost of each link. It can obtain an application-layer multicast tree which is near-optimal solution during the process of solving the problem by the change of relaxation parameter too. We can get the result which is much more closely to the optimal solution. By this way, it′s a simple method to implementation.

2. THE PRESENT MULTICAST TREE GENERATION ALGORITHM IN THE APPLICATION-LAYER ARCHITECTURE

The present multicast tree algorithm can be divided to two kinds: one is heuristic algorithm based on SPT. Its basic idea is that let the single source node be the root, other object nodes be the leaves or the middle nodes. Find an object node which is most closely to the source node by using the shortest path algorithm based on Dijkstra, then add the new nodes and edges into the tree, construct a multicast tree including all of the object nodes gradually. Because the time complexity of Dijkstra is O (*N2*), for |H| nodes adding into the multicast tree, we can know its complexity is O (|*H*|*N2*). It's a simple algorithm to implementation, but we can't make sure that the spanning tree has the minimal cost. The other is the heuristic algorithm based on MST. Prim algorithm is the method we usually used as minimum spanning tree generation algorithm. Its basic idea is that search for a metric value or can be called cost, find the node which is the most closely to the formed tree from the source node, we can know that it has the minimal cost. Add the link and its corresponding notes into the tree, until all the object nodes can be added into it. The time complexity of Prim algorithm is O (*N2*). It's obviously that it adapted to the network with a heavy load. But it may have a longer delay while considering the cost.

3. MATHEMATICAL MODEL OF THE RELATIONSHIP BETWEEN MULTICAST NODES UNDER APPLICATION-LATER MULTICAST[8]

Let the simple undirected weighted graph G (V, E) be the application-layer multicast network establishing on the virtual overlay network. Where V= {1, 2, … n} is the node set of the multicast tree. E= $\{e_{ij}\}$ is the link set of the nodes of multicast tree. For each link e_{ij}, we have the following parameters:

1）let c_{ij} be the cost of using the link e_{ij};
2）let d_{ij} be the needed delay of passing the link e_{ij}

Let d_{ij} be the transmission delay on the link e_{ij}, P={P1, P2,… Pp} be the path set of the network node-pair, delay(s,d) be the delay of the path form node s to node d. According to the discretions above, delay(s, d) can be written as:

$$Delay(s,d) = \sum_{e_{ij} \in p(s,d)} d_{ij}$$

the problem we should solve is that to construct a multicast tree from the multicast source nodes to a group of object node D （D is the object node set）each path from the source node to the object node in tree T should satisfy the delay-constrained and minimum total cost. Let the top limit on the path from source node to object node be Δ . Let delay (T) be the maximum delay of the tree T, cost (T) be the total cost. We can know that the problem should be solved by delay-constrained least-cost multicast routing can be written as: searching for a multicast tree T in the network, satisfying: $Delay(s,d) = \sum_{e_{ij} \in p(s,d)} d_{ij} \le \Delta, d \in D$ (1)

cost-constrained：

$$\min\{\cos t(T) = \sum_{ij \in T} c_{ij}\}$$

Among all the multicast tree satisfying (1)，cost(T) is the minimum cost.

4. APPLICATION OF LAGRANGE RELAXATION IN MULTICAST TREE GENERATION ALGORITHM BASED ON APPLICATION-LAYER

Multicast routing problem with delay-constrained itself is a NP-hard problem. Lagrange relaxation algorithm can deal with combinatorial optimization problem preferably and it is very easy to realize. Many researchers have applied Lagrange relaxation to some combinatorial optimization problem nowadays and get a satisfied result. This paper proposed an algorithm to solve the least-cost multicast tree under the delay constraint condition in the application-layer multicast by introducing Lagrange relaxation.

4.1 Algorithm Description

Multicast routing problem with delay-constrained itself is a NP-hard problem. It absorb cost constrains into the delay function by Lagrange relaxation parameter and change the delay-constrained problem to the optimization problem which has the minimum delay and cost. Its optimization function is:

$$LR(\alpha) = delay(T) - \Delta + \alpha \cdot \min(\cos t(T))$$

Each link generates an aggregate weight function for the cost and delay function on the link in the network. Let the function be: ω=delay+ α ·cost，where α is the relaxation parameter，the optimization function can be written as：

$$LR(\alpha) = \min(T) - \Delta \quad (2)$$

Because Δ is a constant，so the delay-constrained least-cost multicast routing problem can be changed to construct the minimum spanning tree of ω. For a certain α，solving problem (2) is easier than problem (1).

The target value corresponds with the feasible solution of problem (2) is the upper bound of the optimal objective. We can get the lower bound of the minimal value of the object function by choosing the relaxation parameter α （$\alpha \ge 0$ ）. It has been proved that the bigger the value of α, the less cost of the tree, the more delay it has. The minimum spanning tree corresponds with the biggest value of α satisfying delay-constrained is the solution which is the most closely to the optimal solution. We use the sub gradient method to solve such problems: choose a relaxation parameter between minimal delay multicast tree and least-cost multicast tree and amend the value of relaxation parameter α continuously，lessen the set of solution guardedly. Finally we get a delay-constrained least-cost tree.

For two delay-constrained trees with different costs, get the margin of the delays and costs, and then calculate the ratio of them. We can get the value of α according to the ratio. For the two different trees T1、T2，let delay(T1)> delay(T2)，but cost(T1)< cost(T2)，we get ：

$$\alpha = \frac{delay(T_1) - delay(T_2)}{\cos t(T_2) - \cos t(T_1)}$$

We construct a minimum spanning tree T of ω based on Prim algorithm. The process is: choose a node which is the most closely to the tree from the node s. if its delay satisfying the constraints, add it into the tree T, till all of the object nodes be added into it, and then delete the branches which doesn't include the object nodes. The algorithm will be ended by now.

4.2 Specific Steps of the Algorithm

Step1：Construct a minimal cost tree T1 by Prim its root is the source node S. deletes the branches which doesn't include the object nodes. We can get the minimum cost tree T1 from S to object nodes. Compute its delay written as delay (T1). If delay(T1)≤ Δ ，we can know that T1 is the optimum solution to the problem. The algorithm stopped.

Step2：Otherwise store T1 into the solution set T as an optimum tree which doesn't satisfy the delay constrains. (It is known as the optimum infeasible solution).

Step3：Get a minimum delay tree T2 based on Prim. Its root is the source end S. let α =0，construct the minimum spanning tree of ω=delay+ α ·cost or we can say to construct a minimum delay multicast tree, delete the branches which doesn't include the object nodes, and then get the minimum spanning tree T2 of ω, and calculate its cost written as cost(T2). If delay(T2) > Δ ，we can reach the conclusion that it has no solution. Or store T2 into the solution set T, and take it as the optimal solution at present.

Step4：if cost(T2)≠cost(T1), let

$$\alpha = \frac{delay(T_1) - delay(T_2)}{\cos t(T_2) - \cos t(T_1)},$$

ω=delay+ α ·cost, we can get the minimum spanning tree T3 by Prim from the source node S to object nodes for the new weight ω. And then calculate the cost and delay of T2. If cost(T3)＝cost(T1) or cost(T3)＝cost(T2)，we can reach the conclusion that it has no better solution. The algorithm stopped. Otherwise if delay(T3)≤ Δ ，let T2＝T3，store T3 into the solution set T；if delay(T3) > Δ ，let T1＝T3.

Step5：If cost(T2)＝ cost(T1)，the algorithm stopped. Or turn to Step4.

5. SIMULATION EXPERIMENT RESULT

For the network topology model with six nodes (as shown in fig 1), we conduct the simulation experiment according to the algorithm above-mentioned. The link

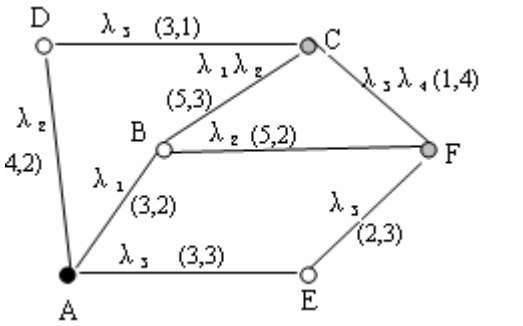


Fig.1. network topology model

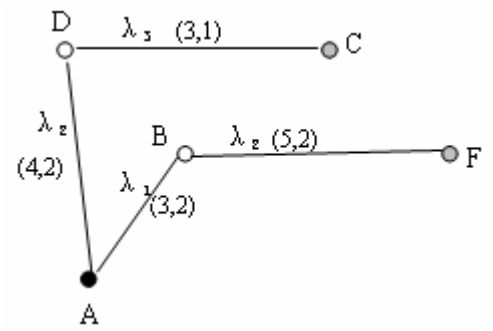


Fig.2. minimum cost tree T1

between the nodes adopts the method of random generation in the simulation experiment and we should make sure it's an always-connected network. Let A be the source node, C.F be the object nodes. We use a binary group (delay, cost) to indicate the value of delay and cost of each link. The purpose is to construct a delay-constrained least-cost multicast tree (maximum delay<=8, or we can say Δ =8).

To construct a minimal cost tree T1 from source node A to object nodes C,F (as shown in fig 2), its delay and cost are delay(T1)=9，cost(T1)=7.

Then construct a minimal delay tree T2 from A to C，F（as shown in fig3），its delay and costs are delay(T2)=6，cost(T2)=10

Because cost(T2)≠cost(T1)，we get:

$$\alpha = \frac{delay\ (T_1) - delay\ (T_2)}{\cos t(T_2) - \cos t(T_1)} = \frac{9-6}{10-7} = 1$$

ω=delay+α·cost=delay+ cost

update the aggregate weight of each edge in fig 1 according to the value of ω above, and construct the minimum spanning tree T3 according to the new weight ω（as shown in fig 4）,where delay(T3)=8，cost(T3)=9.

Because delay(T3)≤8,let T2=T3.We obtain

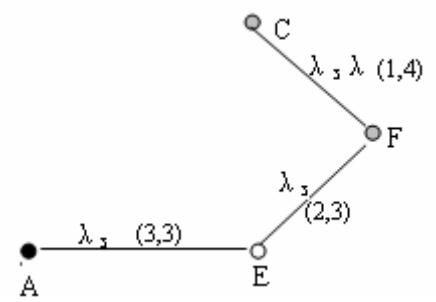


Fig.3. minimal delay tree T2

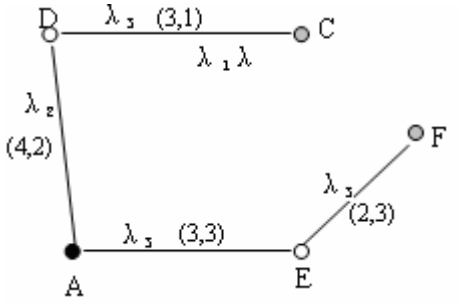


Fig.4. minimum weight spanning tree

$$\alpha = \frac{delay\ (T_1) - delay\ (T_2)}{\cos t(T_2) - \cos t(T_1)} = \frac{9-8}{9-7} = \frac{1}{2}$$

$\omega = delay + \alpha \bullet \cos t = delay + \frac{1}{2}\cos t$ .We can get the minimum spanning tree T3 according to the value of ω (as shown in fig 4). The algorithm cease. Tree T3 is the final result as shown in fig 4.

6. CONCLUSIONS AND DISCUSSION

Lagrange relaxation algorithm is a method of calculating the lower bound for solving combinatorial optimization problem. LR problem includes less constrains so it's easy to be solved. This paper analyzed the delay-constrained multicast routing problem based on the application-layer in the Internet and proposed the algorithm of constructing a delay-constrained least-cost multicast tree based on Lagrange relaxation. Lagrange relaxation was first introduced to the algorithm then adds the cost function into the delay function. The author reduces the complexity of the delay-constrained least-cost multicast tree problem to the minimum spanning tree of function w issues by updating the object function. Finally it can get a near-optimal solution multicast tree. The simulation examples above verified its validity.

REFERENCES

[1] Chuanhe Huang, Xinmeng Chen, Xiaohua Jia, Wentao Zhang; "A Distributed Routing and Wavelength Assignment Algorithm Satisfying Delay and Delay Variation Bound for Multicast in WDM Network;" *Computer Engineering and applications*； 2003，039(022), pp.168-173.

[2] Riabov A, Liu Z, Zhang L. "Overlay multicast trees of minimal delay." In: *Proc. of the 24th Int'l Conf. on*

Distributed Computing Systems. 2004. 654661. http://www.informatik.uni-trier.de/~ley/db/conf/icdcs/icdcs2004.html.

[3] Broash E, Shavitt Y. "Approximation and heuristic algorithms for minimum delay application-layer multicast trees." In: *INFOCOM 2004, the 23rd Annual Joint Conf. of the IEEE Computer and Communications Societies.* Vol 4, 2004.26972707. http://www.ieee-infocom.org/2004/Papers/56_1.PDF.

[4] Banerjee S, Kommareddy C, Kar K, Bhattacharjee B, Khuller S. "Construction of an efficient overlay multicast infrastructure for real-time applications." In: *INFOCOM 2003, the 22nd Annual Joint Conf. of the IEEE Computer and Communications Societies*. Vol 2, 2003. 15211531. http://www.informtik.uni-trier.de/~ley/db/conf/infocom/infocom2003.html.

[5] Tan SW, Waters G, Crawford J. "A survey and performance evaluation of scalable tree-based application layer multicast protocol." *Technical Report*, No.9-03, Canterbury: University of Kent, 2003.

[6] X.-D. Hu and T.-P. Shuai ，Xiaohua Jia，Mu-Hong Zhang；"Multicast Routing and Wavelength Assignment in WDM Networks with Limited Drop-offs;" *IEEE Infocom*; 2004.

[7] Yinzhu Zhou and Gee-Swee Poo; "A New Multi-wavelength Multicast Wavelength Assignment (MMWA) Algorithm in Wavelength-Routed WDM Network;" *IEEE Communications Society*; 2004， pp.1786-1790.

[8] Min Ran, Suixiang Gao, Bao Xu；A Delay-constrained Multicast Routing Algorithm in WDM Networks； Computer Engineering and applications；2005，41(11), pp.119-120.

[9] Heng Wang, Hua Wang, Yamin Sun; "A Delay-constrained Multicast Routing Algorithm Based on Lagrange Relaxation;" *Journal on Communications* 2004, 25(5), pp.83-92.

[10] Kunw adee Sripanidkulchai, Bruce Maggs, HuiZhang. "An analysis of live streaming work loads on the Internet" [C].In: *Proc of ACM SIGCOMM Conf. Internet Measurement*. New York: ACM Press,2004, pp.41-54.

A Dynamic QoS Application Level Multicast Routing Algorithm*

Dezhi Wang [1,2], Zhenwei Yu [2], Jinying Gan [3], Deyu Wang [3]
[1]Department of Computer and Science, North China Institute of Science and Technology
[2]School of Mechanical Electronic & Information Engineering, China University of Mining and Technology
[3]Department of Electrical & Information Science Engineering, North China Institute of Science and Technology
Beijing, China
Email: wangdz20017@sohu.com

ABSTRACT

The multiple QoS constraints multicast routing is a complicated problem. In allusion to the application level multicast (ALM) routing problem with multiple QoS constraints, a distributed dynamic application level multicast routing algorithm was presented. In the algorithm, the network node only need maintain local state information of network links and nodes, and not require the global network state information. The algorithm adopts a dynamic and distributed method to solve the problem. Accordingly, it can satisfy the multiple QoS constraints and get the minimal cost tree. Simulation results show that it has less delay and minimal cost of the tree. It is fitter for network situations with the status changed frequently and multiple real-time multimedia applications.

Keywords: Dynamic, Routing, QoS, Multicast.

1. INTRODUCTION

The multicast is an effective communication way for the computer network from one point or many points to many points. With the increase application of VOD, video meeting, computing cooperate and so on, the multicast is becoming an important technology for network communication [1]. For overcoming the disadvantage of the IP multicast, the application level multicast (ALM) was presented in recent years. The ALM adopts the Internet as the based structure to provide multicast services for end hosts and all multicast packets of ALM transmit in unicast. In the ALM, the end hosts organize an overlay network on the base physical network and multicast packets distribute in the multicast tree on the overlay network. Comparing with IP multicast, the ALM has easy deployment characteristic and solves the address problems. It can implement reliability easily. But its efficiency is lower than IP multicast. Its stability is affected by the capability of the hosts.

The generic application level multicast routing protocols provide the best-effort data traffic. They can not offer quality-of-service (QoS). Those protocols are composed based on the connectivity between the hosts. When the resources of the network are not enough, those protocols can not satisfy the request of the application services. But, with the various application services appearing, the provision of QoS guarantees is of utmost importance for the development of the multicast services. The design of a good multicast routing algorithm is essential for offering effective QoS guarantees on the ALM.

Currently, various projects [2-4] of the ALM are implemented for different application objects and the typical schemes are the Narada, Scatercast, Overcast and ALMI. Among of them, the Narada and Scattercast want each member of the multicast group has the least delay. And the object of the Overcast is to let the each member of the multicast group has the most bandwidth used. The ALMI try to improve the using ratio of the network with reducing cost of the system. But those algorithm do not consider the QoS constraints, they can not provide better QoS. And they need get whole state information of the network or adopt centralized static algorithms. When the network scope increases, they can not expand well.

Some algorithms [5] provide heuristic solutions to the QoS constrained multicast tree problem, which is to find the delay-constrained least-cost multicast trees. These algorithms however are not practical in the Internet environment because they have excessive computation overhead, require knowledge about the global network state, and do not handle dynamic group membership [6]. For instance, QoSMIC dose not eliminate the flooding behavior. It relies on flooding to find a feasible tree branch to connect a new member.

In this paper, we study the delay, delay-jitter and node degree constrained low cost QoS multicast routing problem which is known to be NP-complete, describe a network model for researching the routing problem, and present a distributed dynamic application level multicast routing algorithm with QoS constrained (QDDMR). This algorithm only need maintain partially local state. In QDDMR, a multicast group member can join or leave a multicast session dynamically. The QDDMR can significantly reduce the overhead of constructing a multicast tree

2. MULTICAST OVERLAY NETWORK (MON)

2.1 MON

The ALM tree is constructed by the network hosts which not only receive multicast data, but also replicate and transmit data to other hosts. Because the ALM nodes communication is based on the unicast above the foundation network, any two ALM tree nodes can connect each other. For an overlay network with N nodes, it has $N(N-1)/2$ links. On the one hand, when the network scale N increases linearly, network links will rise in geometry series. The network maintenance state is much more than before. And the algorithm complication also rises. On the other hand, because the network is completely connected, the ALM tree structure may be a star topology based on the shortest path between tow nodes on the ALM tree. The multicast source node is direct connected with all destination nodes, which is same as the unicast communication. From the end host point, this way has the least delay, but global network cost increase greatly. This can not exhibit multicast merit. From the network topology, for network maintenance state, each node must reserve the global network state. This make network extend restrictedly.

In this paper we adopt overlay network technology [7], and construct a multicast overlay network (MON). In MON, the nodes are ALM nodes which do not reserve global network state, and only need maintain neighbor state partly. The MON suppositional link selected principle is that when the suppositional link between MON nodes is a real link in the foundation network, and dose not include the other shortest

* This work is partially supported by the Ph.D. Programs Foundation of Ministry of Education of China #20030290003.

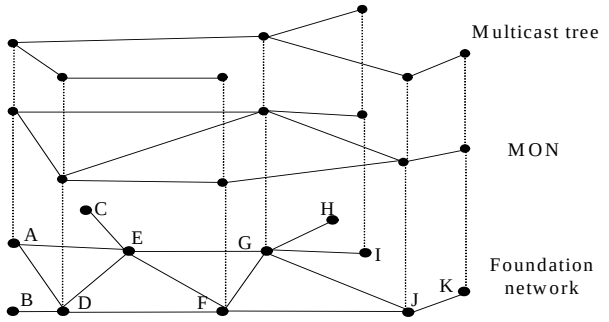


Fig.1. Network topology

suppositional link, this link is reserved. Otherwise this link is deleted. Based on the MON link selected principle, on the normal application layer network we can create a new optimized MON, which link size is much less than a completely connected network. As MON indicated in Figure.1, because the suppositional link between F and K node includes the shortest link of the F, J and K, this link is deleted. However, the links of the F, J and K do not include other shortest links, these links are reserved. By this way, a suppositional link between two nodes is the real shortest path in the foundation network. While the delay and links size reduce, the network cost also decreases. Based on the MON, the ALM tree will has a better performance

2.2 MON Model

An overlay network is modeled as an undirected graph $G=(V,E)$, where V is the set of the source and all destination nodes of the multicast session, and $\forall e \in E$ is the set of the suppositional links on the overlay network. Let $d(e): E \to R^+$ is the link delay, $dj(e): E \to R^+$ is the link delay-jitter, and $P_T(s,v)$ is a path from the source node s to destination node $v \in U$ ($U=\{V-\{s\}\}$ is a set of destination nodes). The path delay, delay-jitter, and cost of the $P_T(s,v)$ can be denoted as:

$$Delay(P_T(s,v)) = \sum_{e_i \in P_T(s,v)} d(e_i),$$

$$Delay\_jitter(P_T(s,v)) = \sum_{e_i \in P_T(s,v)} dj(e_i),$$

$$Cost(P_T(s,v)) = \sum_{e_i \in P_T(s,v)} c(e_i).$$

In above formulas, $c(e): E \to R^+$ is the link e cost. The end host has limited capability of computing and bandwidth, and each host only can be connected with finite other nodes. Therefore, the number of nodes connected with node v can be denoted as $Degree(v) \in N$, $v \in V$.

For multicast services, e.g. VOD and online meeting, the delay and delay-jitter are important QoS constraint parameters. Because of the limited connection capability of the host, the node degree constraint is also absolutely necessarily constraint parameter. So constructing an ALM tree on the MON is searching a tree $T(s,U)$, which satisfies with the following QoS constraints, and make the tree cost minimal.

Delay constraint:

$$Delay(P_T(s,v)) \le D, \quad \forall v \in U \tag{1}$$

Delay-jitter constraint:

$$Delay\_jitter(P_T(s,v)) \le J, \quad \forall v \in U \tag{2}$$

Node degree constraint:

$$Degree(v) \le d_{\max}(v), \quad \forall v \in V \tag{3}$$

Object function:

$$Cost(T) = Min(Cost(T(s,U))) \tag{4}$$

In above formulas, the parameter D, J and $d_{\max}(v)$ are delay, delay-jitter, and node degree constraint values. The delay parameter is close associated with the delay-jitter parameter. The latter a certain extent reflects the stability of the former. They all have addition characteristic. The node degree constraint can balance network load, and make node resource is utilized much more reasonably.

3. QDDMR ALGORITHM

In the QDDMR, the multicast tree construction is driven by the end host, and gradually created. By the state of the suppositional links, the node can know delay, delay-jitter and cost values of the links which are directly connected with itself. For conveniently describing the QDDMR, we bring forward following definitions.

Definition 1: If a path from a new node w to the source node s satisfies with the following formula, the path $P(s,w)$ will be a feasible path for node w joining the multicast tree $T(s,U)$.

$$\begin{aligned} &(Delay(P_T(s,w)) = (d(s,*) + d(v,w)) \le D) \cap \\ &(Delay\_jitter(P_T(s,w)) = (dj(s,*) + dj(v,w)) \le J) \cap \\ &(Degree(s) \le d_{\max}(s)) \cap (Degree(*) \le d_{\max}(*)) \cap \\ &(Cost(P_T(s,w)) = Min(Cost(P(s,w)))) \end{aligned} \tag{5}$$

In the formula (5), the $d(s,*)$ and $dj(s,*)$ are the sum of delay and delay-jitter from source node s to any middle "$*$"node.

Definition 2: If a path $P_T(s,w)$ satisfies with the following formula, the path is an optimization path from the source node s to the new node w.

$$\begin{aligned} &(Delay(P_T(s,w)) = (d(s,*) + d(v,w)) \le D) \cap \\ &(Delay\_jitter(P_T(s,w)) = (dj(s,*) + dj(v,w)) \le J) \cap \\ &(Degree(s) \le d_{\max}(s)) \cap (Degree(*) \le d_{\max}(*)) \cap \\ &(Cost(P_T(s,w)) = Min(Cost(P(s,w)))) \end{aligned} \tag{6}$$

In the QDDMR, firstly the multicast source node is selected as the initialization multicast tree. Then based on the joining or exiting request of the multicast group members, the tree branches are dynamically created or pruned with the corresponding operating principle. Forming a multicast tree process is just a course of the group member joining or exiting process.

3.1 Node Joining

Let new node w is preparing to join the multicast group. The node v is an upriver node directly connected with node w, and the node u is the upriver directly neighbor of node v on the MON.

1) When node w will join a multicast group, it firstly sends a "Join" message to the node v, and node v transmits the message to the node u.
2) Then node u comes into computing test process based on the following formula (7).

$$\begin{aligned} &(d(w,v) + d(v,u) \le D) \cap (dj(w,v) + dj(v,u) \le J) \\ &\cap (Degree(u) \le d_{\max}(u)) \end{aligned} \tag{7}$$

If the formula is satisfied, the node u still transmits "Join" message to its upriver directly connected neighbor node. This process persists until the source node s receives the message.

3) After the message is received, the source node s comes into computing test process based on the formula (5). If the formula is satisfied, node s returns a respondent message "Accept" to the new node w.When node w receives the "Accept", the new node joining process is over, and can receive multicast data.
4) If the following formula (8) is satisfied in the searching routing path process, the node u sends "Reject" message to the downriver node v. Then node v will come into the selecting routing process.

$$(d(w,v)+d(v,u)>D)\cup(dj(w,v)+dj(v,u)>J)\cup(Degree(u)>d_{\max}(u)) \quad (8)$$

5) In selecting routing process, node v sends "Request" to its neighbor nodes except node u. If a neighbor node can still accept a new link, it will return a message "Respond" to node u. Otherwise, it deserts the message and rejects response. If node v receives some "Respond" messages, it selects the fastest response neighbor node as a new upriver node and transmits the "Join" message to it. The joining process still works until a new node is connected with the multicast tree.
6) In selecting routing process, several feasible paths whose "Respond" messages were received by the node v at the same time may emerge. In this condition, node v comes into test computing based on the formula (6). The path which satisfies QoS constraints and has the minimal path cost will become a new multicast routing path. Then the new node continues the joining process.

Algorithm QDDMR_Join(G_{ON}, s, w)
If u satisfies the formula as
$(d(w,v)+d(v,u)\le D)\cap(dj(w,v)+dj(v,u)\le J)$
$\cap(Degree(u)\le d_{\max}(u))$
Then Transmit the Join/Request message to the source s.
Else v sent the Request to its upriver neighbors. End if
While $\forall g\in Neighbor(v)$ Do
If g satisfies the formula as
$(d(w,v)+d(v,u)>D)\cup(dj(w,v)+dj(v,u)>J)$
$\cup(Degree(u)>d_{\max}(u))$
Then Transmit the Join/Request to the source node s.
Else g reject to transmit the Request message to s.
End if .End while.
s receives multiple routing path from w to s.
While all path $P(s,w)$ Do
If $P_T(s,w)$ satisfies $cost(P_T(s,w))=min\{cost(P(s,w))\}$
Then Select the path $P_T(s,w)$ as the multicast routing path.
Else delete the path $P(s,w)$ .End if. End while.

Fig.2. QDDMR_Join algorithm

Other new nodes also iterate above node joining process, and finally construct a new application multicast tree which is satisfied with delay, delay-jitter and node degree constraints, and has a minimal (or near minimal) tree cost. The node joining algorithm is described as the Fig.2.

3.2 Node Exiting

1) If the node which wants to exit the multicast group is a leaf node, it sends a "Prune" message to its upriver directly connected father node.
2) When upriver father node receives the message, it prunes this branch from itself to the son leaf node. And a leaf node exiting process is over.
3) When an exiting node is a non-leaf node, because all ALM tree nodes are also multicast group members, the son nodes of the exiting node still need be connected with the tee after their father node exits the tree. Therefore, when the exiting node sends a "Prune" message to its father node, it must send other "Prune" messages to its son nodes and tell them their grandfather's address.
4) While the upriver father node receives the "Prune" message, it prunes the branch from itself to the son non-leaf node. So a non-leaf node exits the ALM tree.
5) While a son node of the non-leaf node receives the "Prune" message, it sends a "Join" message to its grandfather node whose address is got from the "Prune" message. The son node requests joining the tree, and implements a new node joining process again. In the end, all son nodes will rejoin the tree. The node exiting algorithm is described as the Fig.3.

Algorithm QDDMR_exit(T, s, w)
w sends the Prune to the father node v in the tree.
If w is not the leaf node of the tree
Then w sent the Prune message to its children nodes. End if
v delete the child w after it receives the Prune of the w.
If v is a relaying node.
Then v transmits the Prune to its father. End if
Children rejoin the tree after received the Prune from w.

Fig.3. QDDMR exit algorithm

4. SIMULATIONS

In this section, we discuss the simulations and performance of the QDDMR for the ALM routing problem with multiple QoS constraints. For better performance evaluation compare of the algorithm, we also simulate the other algorithm YAM, QMRP, and this paper algorithm QDDMR. The network simulation platform is Network Simulator 2.0. The network topologies used in the simulations experiments are manipulated to simulate wide area sparse network. The network graphs used in the simulations are constructed by the Waxman's random graph model. In each experiment, a source node and destination nodes are random selected. Every experiment is repeatedly done 50 times, and takes the average value of all experiments as the final result. Thereby the experiment results are much more authentic.

In experiments, the multicast service delay constraint varies in the bound $[0.5s, 2s]$, and the delay-jitter constraint is in the bound $[0.5s, 1.5s]$. With the network nodes increase, QoS constraints are broadened accordingly. The node degree constraint varies in the bound $[1,4]$. Each node degree is random selected, but the sum of all the node degree value is $(|V|-1)$. Thereby network bandwidth is sufficiently used.

In Fig.4 the lines are the results of the multicast tree cost with the group size increase. From the figure, we can analyse that when the multicast group size increases, the cost of the QDDMR, YAM, QMRP also rise. But the increase range of the QDDMR is the least. And the cost of the QDDMR is also the least with the same group size. So the QDDMR can search a much better reasonable routing path and optimizes the tree cost in the same condition relative to other two algorithms.

In Fig.5, the lines are the variety results of the searching path successful probability of the three algorithms with the

group size increase. From the figure results, the probability

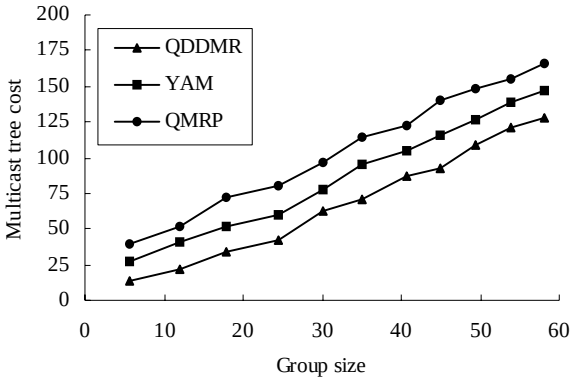


Fig.4. Multicast tree cost compare

increases with the group size variety because while the network scope expands, the candidate path size also increases, that make the probability increase. In the same network scope, the QDDMR also has a maximal successful probability because this algorithm adopts the divided path searching way which can much faster find a branch routing path and get an upper probability.

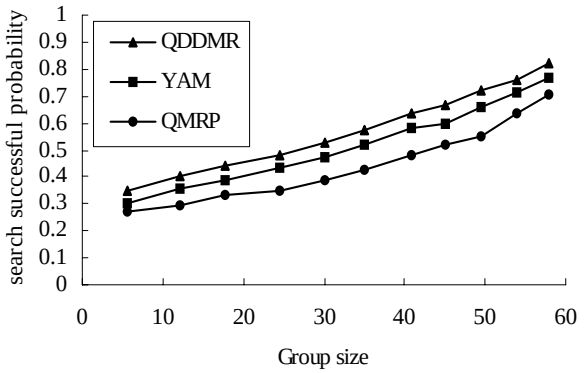


Fig.5. Search path successful probability

5. CONCLUSIONS AND FUTURE WORK

Currently, the multiple QoS constraints multicast routing problem is a hot point of the computer network research. In this paper, we deeply study the ALM routing algorithm with delay, delay-jitter and node degree multiple QoS constraints, construct a new network model based on the special MON, and present a new distributed dynamic ALM routing algorithm QDDMR with multiple QoS constraints. The algorithm can connect a new node with the tree in an optimization or near optimization routing path based on dynamic divided searching feasible branch paths. The QDDMR can effectively reduce the overhead of constructing the tree with multiple QoS constraints. In the QDDMR, a multicast group member can join or leave a multicast session dynamically, which dose not disrupt the existent multicast tree. Simulation results show that QDDMR works simply, has better expansibility, and is an available approach to multicast routing decision with dynamic group topology.

Our work is just beginning, only has some limited testing and simulation. The design needs to be validated in actual using. It is necessary to do more optimize for some multi-objective problem during the process of looking for the best multicast trees in the future.

6. ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their thorough comments.

REFERENCES

[1] C.K. Yeo, B.S. Lee, and M.h. Er, “A framework for multicast video streaming over IP networks”, *Networks Compute*. Rev. Lett., Vol.26, 2003, pp. 273-289.

[2] Jannotti J, Gifford D, Johnson K. “Overcast: Reliable Multicasting with an Overlay Network”, in *Pro. Proceedings of the Fourth Symposium on Operation Systems Design and Implementation*, San Diego, CA, 2000, pp. 197-212.

[3] D. Pendarakis, S. Shi, D. Verma, M. Waldvogel, “ALMI: an Application Level Multicast Infrastructure”, *in Pro. Proceedings of the Third Usenix Symposium on Internet Technologies and Systems* (USITS), March 2001.

[4] Y. D. Chawathe, “Scattercast: an architecture for Internet broadcast distribution as on infrastructure service”, PhD Thesis. Stanford University, Sep 2000.

[5] Chen S, Nahrstedt K, Shavitt Y, “A Qos-aware multicast routing protocol”, *IEEE Journal on selected areas in communications*, Vol.18, 2000, pp.2580-2592.

[6] Li Layuan, Li Chunlin, “A QoS multicast routing protocol for dynamic group topology”, *Information Sciences*, Rev., Lett., Vol.169, 2005, pp.113-130.

[7] Yunxi, Sherlia, Shi, “Design of Overlay Networks for Internet Multicast”, *PhD thesis*. Washington University, 2002.

Dezhi Wang received his B.S degree from the Beijing Institute of Petro-Chemical Technology, China in 2001, and his M.S degree from the Liaoning Technical University, China in 2004. He is working toward the Ph.D. degree at the China University of Mining and Technology, China. His research focuses on multicasting, overlay network management, multicast modeling, distribute system and performance evaluation.

Zhenwei Yu is a Professor in the China University of Mining and Technology, China. He was ever the chief of the ISCA computer network conference. His research interests include network architecture, overlay networks and multimedia networking.

Analysis of Fairness and Utility of the User's Consumption in the TCP Networks*

Xianfang Wang[1,2], Kunhua Zhu[1], Zhiyong Du[3]
[1]Department of Information and Engineering, Henan Institute of Science and Technology
Xinxiang, Henan 453003, P.R.China
[2]School of Information & Control Engineering, Southern Yangtze University
Wuxi, Jiangsu 214122, P.R.China
[3]Henan Mechanical and Electrical Engineering College, Xinxiang 453002, P.R.China
Email:[1]wangfang@163.com

ABSTRACT

This paper deals with the fairness of pricing scheme in TCP network and how the users to modulate rate to achieve the best utility As the case of a single bottleneck. The incentive Stackelberg strategy concept was introduced to the model of network system to make the users to obtain the best rate. At the meantime, the strategy can prevent the users from occupying their resource of the network excessively, which can avoid the congestion of the network to a certain degree. Finally, some numerical simulations about nonlinear strategy are given via MATLAB to illustrate the proposed method. The result of the simulation certifies the validity and practicability.

Keywords: Pricing Scheme, Fairness, A Single Bottleneck, Incentive Stackelberg Strategy

1. INTRODUCTION

With the expansion of the bandwidth and the increasing number of users, they, the network designers, are facing a grim problem-how do they provide a fair and effective allocation for the available bandwidth. In the recent network, there are so many connections are using TCP(Transmission Control Protocol) such as FTP、HTTP、DNS、SMTP etc. TCP retains two state variables: cwnd and ssthresh to control the transfer speed. The latter used to distinguish slow start from congestion avoidance. The source end adopts the method of increasing the value of cwnd by the index way at a first stage of establishing the connection till the data packet loss. When it comes TCP-Reno will halve the value of ssthresh. When cwnd obtain the new value of ssthresh, TCP enter upon a phase of congestion avoidance, cwnd will increase by the linear way soon after. This kind of mechanism estimates the available bandwidth by ssthresh and detects the additional bandwidth by the method of congestion avoidance. Nevertheless, TCP no need for giving a fair and effective allocation for the available bandwidth in the connection.[1] The researchers have proposed many different rate allocation mechanism so far, for instance, the perceive flow control mechanism based on RTT was first proposed by Nandy et al[2] and ECN (Explicit Congestion Notification) was adopted by Matsda et al[3] to solve such fair problem.

The network is a public industry in fact and the potential uncooperative conditions also stimulate the researchers to dig out more strategy. Nowadays it is considered that the system optimal problem can de divided into two facets- the network and the users by Kelly's study. Systems try to achieve the best optimization for the user's selective consumption and the allocation of the rate[4]. We should consider the fairness of the user's rate allocation; moreover try to maximize the user's utility as much as possible.

* Project name: Wireless mobile computer equipment based on Bluetooth, NO: 863-306-ZD13-04-8

2. THE FAIRNESS OF PRICING SCHEME

Congestion control algorithm based on the window not only needs to control the transmission speed, it also limits the maximum quantity of the unreleased packets according to the congestion window. It favors to ease the problems causing by the users′ inaccurate forecasts of the available bandwidth. The throughput of the connection relies so much on its RTT, it is bad for sharing the bandwidth fairly at the junction of the bottleneck. Suppose the user adopt the rate-based congestion control algorithm, and if they can not forecast available bandwidth accurately and thus put the dada packets into the network with a very high speed, then the network will lost the packets with a high rate because of over-load buffer, and it takes a long time to recovery[5]. in the open network, it can guarantee the network stability by controlling the number of the packets and the connection and then assure no user can increase the rate arbitrarily because of the users′ inaccurate forecasts of available bandwidth and take it as a penalty for other users during the network congestion. If the total rate of a link is less than the bandwidth capacity of it, there is no congestion, and every user can reach his expected speed so need not to compete with the other users. Otherwise, it can cause the overstock in the source end if any user attempt to accelerate their own rate when the total rate reached the bandwidth capacity of the link, and then it can lead to a serious queue delay. Suppose the network attempt to increase the consumption of the system while a queue delay, as we seen in the flowing pricing scheme：

Let e_j be an overstock queue length of source end j, $j \in J$ .when the total rate passing the source end is less than the bandwidth capacity of the link, we can suppose that it has no congestion. When source $j \in J$ has congestion, we can know that the total rate passing it equals to the bandwidth capacity of the link, it need to cost a price in the source end at the moment.

The cost of per-unit flow λ_j is the cost caused by the queue delay of the source end. $\lambda_j = e_i / C_j$ .so we can get the total price of per-unit flow on router $J \in J_i$ is $\sum_{j \in J_i} \lambda_j$ .let the rare of use i be x_i , we can get that the user i spend $x_i \bullet \sum_{j \in J_i} \lambda_j$ per second because of the delay. Therefore, we have the user's utility function or we can say node beneficial

function as flowing:

$$U_i(x_i) - x_i \bullet \sum_{j \in J_i} \lambda_j = U_i(x_i) - x_i \bullet \sum_{j \in J_i} \frac{e_j}{C_j} \quad (1)$$

Considering the cost of per-unit flow, the users only need to know the total cost of per-unit on its router instead of the cost of the source end, for maximizing the object function. Now let's introduce how the users use TCP to calculate the cost of per-unit flow without the help of network. We suppose that every connection knows its propagation delay in the router, it can be realized by keep detecting the RTT of the packet Let the object queue length of the user's be $p = (p_i, i \in I)$, and the user's window size is close to the equilibrium point of TCP [6], what is more, the rate now satisfying the weighted scale average, we can get the per-second cost as flowing:

$$d_i = x_i \bullet \sum_{j \in J_i} \frac{e_j}{C_j} = \sum_{j \in J_i} e_j \bullet \frac{x_i}{C_j} = \sum_{j \in J_i} e_j^{\,i} = p_i \quad (2)$$

Where $e_j^{\,i}$ is the queue length of connection *i* in source *j*. We suppose the sending rate of every link happened to be the queue length of congestion in the source end. This accords with the service discipline of FIFO of switches .therefore, for a definite point p, the user's cost equals to its queue length, what is more, the user can speculate their own cost according to the object queue length.

One important aspect of pricing scheme is fairness. The cost of a connection in source $j \in J$ should be equal to its rate. In other words, the cost of per-unit flow for each connection in the source end should be the same. So it is easy to see form the pricing scheme above, when a new user enters the network, its cost equals to the total increasing of the cost of the system. The cost of new user i equals to its object queue length p. we can calculate the total cost per second of the system as flowing:

$$\sum_{j \in J} C_j \bullet \lambda_j = \sum_{j \in J} C_j \bullet \frac{e_j}{C_j} = \sum_{j \in J} e_j = \sum_{i \in I} p_i \quad (3)$$

Thus, the fairness of pricing scheme is protected automatically.

3. THE APPLICATION OF PRICE INCENTIVE STRATEGY IN THE USERS'RATE MODULATION

It has been mentioned in Kelly's references that the unit price of the flow is an intermediate variable. The system optimization can be realized when achieving a balance between the user's cost choice and the choice of the distributive law of the network [7]. In the game theory model its input was controlled respectively by at least two players so that the system status can reach their won requested output. So the game theory afforded an architectural structure to analyze the dynamic characteristics of the uncooperative network [8].

3.1 System Model

We consider a network with a resource set J, let C_j be the band-limited capacity of resource *j*, and *j* is a member of the set *J* . The users in set I use the network at a speed of $x = (x_1, x_2, \cdots, x_i)$. We can get the maximum utility model for each user I as following:

$$USER_i(U_i, \lambda_i):$$

$$\text{Maximize:} \quad U_i(\frac{p_i}{\lambda_i}) - p_i$$

$$\text{Over:} \quad p_i \geq 0 \quad (4)$$

Where λ_i is the unit price of the flow per second $x_i = \frac{p_i}{\lambda_i}$ is the user's rate, the utility function U_i is a continuously derivable and strictly convex increasing function when $p_i \geq 0$.

Now, we can reach some conclusions about the optimal problem of the system as follows:

$$NETWORK(A, C, p):$$

$$\text{Maximize:} \quad \sum_i p_i \log x_i$$

$$\text{Subject to:} \quad A^T x \leq C$$

$$\text{Over:} \quad x \geq 0 \quad (5)$$

Where A is a 0-1 matrix.

Theorem: For a set $T : P \to P$

$$T_i(p) = \arg\max_{\tilde{p}_i} U_i(\frac{\tilde{p}_i}{\lambda(p)}) - \tilde{p}_i \quad (6)$$

Where $P = R_+^I$, $\lambda(p)$ is a unit flow vector which in the vicinity of an independental fixed stable point of TCP. There exist a fixed point p_i^* satisfying the mapping T , the rate allocation x_i^* is the best rate at the point p_i^* , at the meantime, and it's the solution to $SYSTEM(U, A, C)$. Problems above-mentioned satisfy:

(1) $p_i^* = x_i^* \bullet \lambda_i^*$;

(2) x_i^* is the solution to $NETWORK(A, C, p)$;

(3) p_i^* is the solution to $USER_i(U_i, \lambda_i)$.

Tack the partial derivative of $U_i(\frac{\tilde{p}_i}{\lambda_i^*}) - \tilde{p}_i$, we get

$$\frac{\partial}{\partial \tilde{p}_i}\{U_i(\frac{\tilde{p}_i}{\lambda_i^*}) - \tilde{p}_i\} = \frac{1}{\lambda_i^*} U_i'(\frac{\tilde{p}_i}{\lambda_i^*}) - 1 \quad (7)$$

According to Kunhn-Tucker, this is a sufficient and necessary condition, $\tilde{p}_i$ satisfy:

$$\tilde{p}_i > 0 \Rightarrow U_i'(\frac{\tilde{p}_i}{\lambda_i^*}) = \lambda_i^*$$
$$\tilde{p}_i = 0 \Rightarrow U_i'(0) \leq \lambda_i^* \quad (8)$$

Therefore, for any equilibrium point p_i^* we get:

$$x_i^* > 0 \Rightarrow U_i'(\frac{p_i^*}{\lambda_i^*}) = U_i'(x_i^*) = \lambda_i^*$$
$$x_i^* = 0 \Rightarrow U_i'(0) \leq \lambda_i^* \quad (9)$$

$$p_i^* = x_i^* \bullet \lambda_i^* = \begin{cases} x_i^* \bullet U_i'(x_i^*) & x_i^* > 0 \\ 0 & x_i^* = 0 \end{cases} \quad (10)$$

For such an equilibrium state, if the user I doesn't change the parameter p_i, the rate now will be the user's optimal rate. Hence we obtain the following renewal strategy:

$$p_i(t) = \arg\max_{p_i} U_i(\frac{p_i}{\lambda_i(t)}) - p_i = \begin{cases} 0 & \text{if } \lambda_i(t) > U_i'(0) \\ p_i^* & \text{if } 0 < \lambda_i(t) < U_i'(0) \end{cases} \quad (11)$$

Suppose that the adjustment of price occur within range of a long time, what is more, the users allow their window size closely to the TCP equilibrium point. The user calculates its optimal price based on the current system flow unit $\lambda_i(t)$ at any time to achieve the best utility of the node. The users need to wait till the flow unit price debased if it is too high.

Considering the one-to-one correspondence between the price vector and its corresponding rate allocation, it's a challenging problem that to introduce the user's gathering grade in a common network. In some cases, the users gather in a single bottleneck .the unit price of flow per second are the same. so ,every user adjust its price based on the current system unit price of flow.

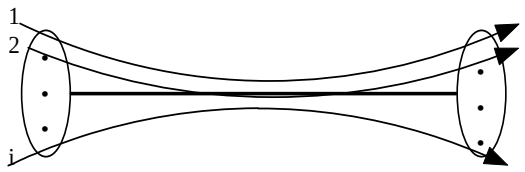


Fig.1. A single bottle neck

Users need to know both available bandwidth and flow unit price in such a situation. It's different to obtain the best rate since the residual available bandwidth can be taken by other users. According to the theorem in reference [9] we can know that Problem (4) exists a Nash equilibrium point in a single bottleneck link with the bandwidth limited capacity and using by limited users .So, the stackelberg strategy in game theory was introduced in the model here .The network system is the host and the users are guest that satisfying Nash equilibrium point and what's more, both the system and users can take the library of changing x_i. As a result, the host must be in the magisterial position if it requests any other user to reach the prescriptive price of the system. We can reach the conclusion according to the following Stackelberg strategy:

$$\xi_i(x_i) = \lambda_i + q_i(x_i) - q_i(x_i^*) \quad (12)$$

Where $q_i(x_i)$ is any one of the uncertain function of x_i. x^* is the expected point to meet the requirement of the user's rate in the network.

$$\xi_i(x_i^*) = \lambda_i \quad (13)$$

$$\text{argmax}[U_i(x_i) - \lambda_i x_i - q_i(x_i)x_i] = x_i^* \quad (14)$$

3.2 The Nonlinear Incentive Strategy

The strategy to stimulate the users to accelerate the speed is taken when the total rate of the link is less than the bandwidth capacity of it, but it will be forced to slow down after it beyond the optimum point .

Consider such a nonlinear function:

$$q_i(x_i) = \begin{cases} \frac{\lambda_i(x_i^* - x_i)}{x_i} & \text{if } x_i < x_i^* \\ 0 & \text{if } x_i = x_i^* \\ \frac{\mu\lambda_i(e^{\frac{x_i}{x_i^*}-1} - 1)}{x_i} & \text{if } x_i > x_i^* \end{cases} \quad (15)$$

Where μ is a penalty divisor which is greater than zero. Replace λ_i in (4) with a nonlinear structure ξ_i ,problem(4)can be written as:

$$\text{Max } W_i(x_i), \quad \text{over } x_i \geq 0 \quad (16)$$

where $W_i(x_i) = U_i(x_i) - \lambda_i x_i - q_i(x_i)x_i$. satisfying both (13) and (14) by checking

4. NUMERICAL EXAMPLES AND SIMULATION RESULT

Choose a utility function such that: $U_i(x_i) = 6\log(x_i + 1)$, let $\lambda = 1$, according to $U_i'(x_i) - 1 = 0 \Rightarrow x_i^* = 12.81$ and $U_i'(0) = 6$, satisfying $\lambda_i < U_i'(0)$, $p_i^* = 12.81 \bullet 1 = 12.81$. The method of network control was taken and Kelly's utility function was introduced to also. Put $q_i(x_i)$ into $W_i(x_i)$ We can point out the curve of $W_i(x_i)$ μ =1, 3, 8 we can reach the conclusion that the downward trend will be much more obvious with the increasing of μ .

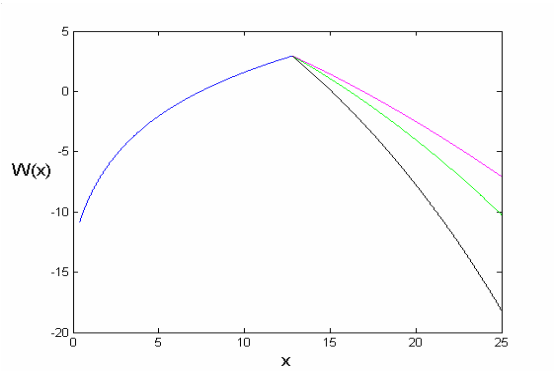


Fig.2. The curve of user's utility function

As shown in graph 2, $W_i(x_i)$ obtain the largest value at the point of $x_i = 12.81$, it is obviously that x=12.81 is a division point. The curve increases slowly in the former part and falls sharply in the other. Therefore the users felt a great necessity to modulate their rate for achieving the best utility .They will make it to approximate to x_i^*, for making the utility function maximize.

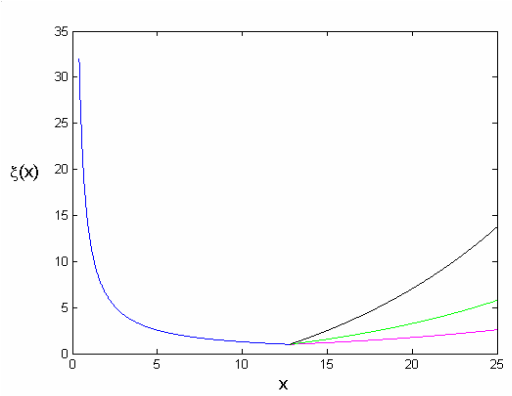


Fig.3. Numerical curve of nonlinear incentive strategy

According to (12), as the case of a nonlinear condition:

$$\xi_i(x_i)=\begin{cases}1+\dfrac{12.81-x_i}{x_i} & \text{if } x_i<12.81\\ 1 & \text{if } x_i=12.81\\ 1+\dfrac{\mu\lambda_i(e^{\frac{x_i}{12.81}-1}-1)}{x_i} & \text{if } x_i>12.81\end{cases}$$

We can reach the result, $h=6$, $\lambda_i=1$, to the contour curve $h\log x_i-\lambda_i x_i$ by graph 3. The broken curve in the picture is the curve of nonlinear incentive strategy $\xi_i(x_i)$ when μ =1, 3, 8. Hence we obtain the max value of the curve is $x_i=12.81$, $\lambda_i=1$.the user can get the greatest utility function at this point. In other words ,comparing with x_i^*, the more approximate the user's rate ,the more benefits they can get ,we can get the following conclusion by picture 2, if the value of x-axis is less than x_i^*, $\xi_i(x_i)$ decreased gradually,这 the lower $\xi_i(x_i)$,the greater the user's rate, however $\xi_i(x_i)$ will be increased when the user's rate is beyond the optimal point x_i^*.This kind of incentive strategy was adopted to encourage the users to adjust their rate, avoid waste of resources and benefit the users at the same time when the network flow is greater then the user's total need. As we can seen that the bigger the penalty divisor μ , the steeper the curve is and the more obvious the incentive application is. We should pay a tension to that the users should adjust the rate in time to avoid t $\xi_i(x_i)$ too high. At the meantime, Debate the rate can relieve the network congestion to a certain degree and can avoid the congestion caused by the total rate beyond the network bandwidth capacity since the over speed of user i. Decrease sharply after the optimal point can avoid the unnecessary cost caused by increasing rate arbitrarily. Every user can use the network at the best rate when the network has limited users and the flow of network is more than the total demand of the user.

5. CONCLUSIONS

This paper analyzed the fairness of pricing scheme TCP network and discussed the uncooperative user's utility problem with the incentive Stackelberg strategy in game theory. Simulation result showed that it is particularly important for both the network and the users to restrain the users to use the network resources more effectively by using this method. In recent years the methods building a model by using the game theory came in increasing numbers for the route planning and flow control in the communication network. Both the specified price by the network administrators and user's reaction rate concern the user's utility and affect the congestion of the network. Therefore, it is hot spots of specifying a reasonable price and using the different strategies for today's network management. It is of great practical significance to combine the price control and the view of market and it is basic to measure the utilization of the network and its gains.

REFERENCES

[1] S Floyd. HighSpeed *TCP for large congestion windows;[S].RFC3649* ,2003.

[2] NANDYB ,SEDDIGHN, PIEDAP, etal, "Intelligen Traffic conditions for assured for warding base Differentiated service networks[A],"in *Proceedings of Hig Performance Networking[C]*,Paris: IFIP, 2000.

[3] MATSUDAT,NAGATAA,YAMAMOTOM.TCP,"Rate control using active ECN mechanism with RTT Based marking probability[A],"in *Proceedings of ICC02[C]*. NewYork:IEEE,2002, pp.981-985.

[4] Medina A, Allman M, Floyd S,"Measuring the Evolution of Transport Protocols in the Internet[J]," *ACM Computer Communications Review*, 2005, 35(2).

[5] T kelly.Scalable,"TCP:improving perfomnance in high-speed wide area network[J],"*ACM computer communications Review*,2003, 33(2),pp83-91.

[6] Yang Yan,Tan Liansheng,Xiong Naixue,*Anovel TCP congestion control algorithm in multipl ebottl eneck link. Mini-MicroSytems*,2005, 26(2), pp.186-191(in Chinese).

[7] M Nabeshima, K Yata,"Improving the convergence time of highSpeed TCP[A],"in *IEEE International Conferenceon Networks[C].Singapore:IEEE*, 2004 ,pp 19-23.

[8] J. B. Rosen,"Existence and uniqueness of equilibrium points for concave n-person games[J],"in *Econometrica*, 1965,33(3), pp.520-534.

[9] Richard J. La and Venkat Anantharam,"Charge-senstive TCP and Rate Control in the Internet[A],"in *Proc. IEEE INFOCOM[C]*,London, 2000, pp.1166-1175.

Xianfang Wang is an associate Professor. Now, she is studying PhD in School of Information & Control Engineering of Southern Yangtze University. Her research interests are in networks of computer, control theory and control engineering.

Study and Simulation of Cell Queuing Time Delay In Optical Access Network System

Hua Liang [1], Guangxiang Yang [1], Dexin Tao [2]
[1] School of Computer Science and Information Engineering
Chongqing Technology and Business University, Chongqing 400067, China
[2] Wuhan University of Technology, Wuhan 430063, China
Email: ygxmonkey@126.com

ABSTRACT

Cell access time delay of ONU (Optical Network Unit，ONU) in BPON (Broadband Passive Optical Network based on ATM) is studied and emulated in this paper. An algorithm of upstream cell time delay and cache length or buffer size in the ONU are given, which is based on the queuing theory of M/G/1/∞ model. Through simulation experiment by using OPNET, CD(Cell Delay) and CDV (Cell Delay Variation) results of CBR and VBR cell streams are acquired. The experimental results show that by using queuing theory of M/G/1/∞, CD and CDV can be reduced and capability of access network can be improved , which would provide higher QoS. The given algorithm in this paper can improve capabilities of Cell Delay and Cell Delay Variation, provide the referenced theory criterion of BPON MAC (Media Access Control) protocol designing.

Keywords: Optical Communication, BPON, Queuing Theory, MAC

1. INTRODUCTION

In passive optical access network based on ATM, there are 32 or more ONU(Optical Network Unit，ONU) who share the network resource. In upstream direction, TDMA (Time Division Multiplex Access) is used to access network[1], so Media Access Control protocol is used to avoid upstream cell collision and provides transparent transmission of multi-service. Arrived cells of subscriber such as voice, data, and video are stored in ONU' buffer, and after waiting time delay, these cells are multiplexed into one data frame in their own upstream time (called time slot) and transmitted to OLT(Optical Line Termination) through fiber. In the access network, cell delay (CD) and cell delay variation (CDV) are two most important characters, which have seriously influence on network capability. Therefore, it can provide applied algorithm for designing of ONU buffer and can improve access network capability by analyzing cell upstream access time delay with queuing theory.

2. QUEUING MODEL OF BPON

Queuing model of broadband passive optical network is illustrated in Fig.1, whose basic character is that ONUs apply the required bandwidth and OLT assigns later according to bandwidth allocation algorithm. In this way, there are no collisions of cells in the line. Ways of applying bandwidth are classified as SR and NSR, it is that ONU reporting status (SR) or OLT monitoring the upstream bandwidth (NSR, non Status Reporting). Each ONU have cell buffers, which are corresponding to the T-CONT of each ONU. Each T-CONT store the different priority service cells, and these cells come into the different T-CONT to wait for being transmitted. To the way of SR, every ONU reports the cell number in each T-CONT by mini-slot at interval (on the assumption that the interval is W, which can be set by OLT with sending Divided-slot grant); To the way of NSR, OLT collects and calculates the total cells number of ONU and its T-CONT (that is the bandwidth of ONU) at interval of W. When OLT gets this information, it may allocate the bandwidth to every T-CONT of ONU by considering of their priority. The downstream bandwidth is indicated by downstream data grants which are stored in the buffer and transmitted in the PLOAM (Physical Layer Operation and Maintenance) cell. When each ONU receive one data grant, they will send one upstream cell at the corresponding data grant time slot. What is described above is access process of BPON.

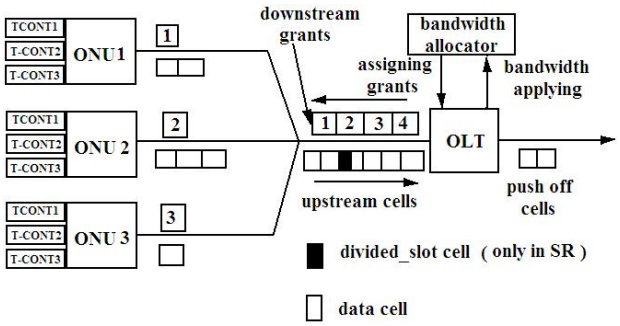


Fig.1. queuing model of BPON

MAC (Media Access Control) protocol is the core of queuing model. Formats of downstream and upstream data frame, time interval and frame format of reporting upstream queuing cells number, downstream grant assigning plan and bandwidth allocating plan are all dependent on MAC protocol.

Source model and its compound stream model can be used to simulate the practical running process of multiple services in BPON. And in this way, performance objectives of BPON can be known in advance. In order to acquire high capability but being irrelevant to service, and reduce the influence of MAC protocol on parameters of BPON QoS (Quality of Service), performance studying should be generalized. Considering these cases described above, cell time delay (CD) and cell time delay variation (CDV) of real time service cell stream, for example, CBR, and non real time service cell stream, for example, UBR which is often represented by ON-OFF model, would be studied on different load condition in this paper, and capability of service in the different priority should also be studied.

On consumption that source stream model will generate cells which comply with Possion distribution. This model can be described and scaled by Possion intensity. There are two advantages when using this distribution to generate cells in the process of computer simulation, one is that there are no aftereffect; the other is that multiple Possion streams when being mixed into one stream still keep the Possion character, and the intensity of compounding streams is the total intensity of all individual Possion stream. As a kind of model of

describing random phenomena, Possion distribution plays an important role in the queuing theories and communication network. In the theoretical analyzing, rules of calculating queue length and cells average time delay are provided by using Possion distribution and queuing model.

3. STUDYING OF BUFFER QUEUE LENGTH

Supposing that cells arrive with Possion distribution, Possion parameter is λ, which indicates that there are λcells arriving within the unit time (one slot in this research). Multi-Possion streams can be compounded into one stream whose parameterλ is sum of each Possion stream, that is λ1+λ2+…+λn. Multi-Possion streams follows the general serving time distribution, that is, M/G/1/∞ queuing system. Cell queuing is analyzing by using M/G/1/∞ model in this paper.

To M/G/1/∞ queuing model, as serving time follows the general distribution, to random selected time point t, the customer which is being served may not finish serving. From t point, the left serving time doesn't follow the former time distribution and may have remembrance. Consequently, the system process would be affected by the former status. Nevertheless, if the left time of customer is especial in M/G/1/∞ model, for example, at time of one customer just being finished, from this moment, the work status of model is just pull round; or at this time system is idle status or begins to serve another customer. The moment of finishing serving may not be the same time as that of customer arriving. To the customer on the road, the arriving time in compliance with the negative exponential distribution, as negative exponential distribution have no remembrance, the left arriving time is still in compliance with the negative exponential distribution. At this moment, system looks just like as recommencing, the following status is decided by the status of this moment, and is irrelevant to former status. This moment is called a second birth point or a second birth time. So all the moments of finishing serving can be found out to buildup a second birth point series, that is: t1，t2，…tn，…$\{t_n\}$ is a random series, the status of model (cells number) have Markov characteristic when being watched on the second birth point[2]. Nn represents the left cells number in the buffer that when the No, n cell leaves. $\{N_n\}$ is a Markov chain, is also called imbedded Markov chain, and $\{N_n\}$is also a homogeneous Markov chain.

Assuming that the probability of reaching k cells in one time slot is α_k (k= 0，1，2，…), and reaching λ cells averagely. Serving time $\frac{1}{\mu}$ is a fixed time slot. Assuming that density function of serving time is $b(t)$, the average serving time is:

$$E[V]=\frac{1}{\mu}=\int_0^\infty tb(t)dt \qquad (1)$$

Laplace transformation $B^*(s)$ of $b(t)$ is:

$$B^*(s)=\int_0^\infty e^{-st}b(t)dt$$

Supposing: $\rho=\frac{\lambda}{\mu}$

C_n : the nth cell of going to ONU buffer;

t_n : the moment of leaving BPON system when finishing C_n serving;

N_n : the queue length when C_n left;

V_n : serving time of C_n;

A_n : arriving cells number within serving time V_n of C_n;

As analyzed above, $\{V_n\}$ is an independent random series and follows the same distribution, its distribution density is $b(t)$, $\{A_n\}$ is an independent random series and follows the same distribution, its probability distribution is $\{\alpha_k\}$.

It can be concluded:

$$\alpha_k=\int_0^\infty \frac{(\lambda t)}{k!}e^{-\lambda t}b(t)dt \qquad (0\le k<\infty) \qquad (2)$$

Average value $E[A_n]$ of A_n, that is, average cells number within the nth cell serving time V_n, is as follows:

$$E[An]=\sum_{k=0}^{\infty}k\alpha_k=\int_0^\infty\sum_{k=0}^{\infty}k\frac{(\lambda t)}{k!}e^{-\lambda t}b(t)dt=\int_0^\infty\lambda tb(t)dt=\rho$$

$$D[A_n]=\lambda^2D[V]+\rho$$

The transition-probability matrix is:

$$P=(p_{ij})=\begin{pmatrix} a_0 & a_1 & a_2 & a_3\ldots\ldots \\ a_0 & a_1 & a_2 & a_3\ldots\ldots \\ 0 & a_0 & a_1 & a_2\ldots\ldots \\ 0 & 0 & a_0 & a_1\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & \end{pmatrix}$$

It can be concluded by transition matrix P that $\{N_n\}$ is a homogeneous Markov chain, is aperiodic and irreducible. On condition that $\rho=\frac{\lambda}{\mu}<1$, this Markov chain has character of ergodicity, so the stationary distribution exists. Status transition figure is as Fig. 2.

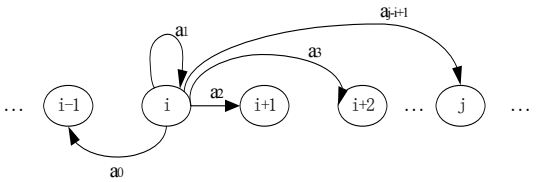


Fig.2. Markov status transition Figure

Because $\{p_j\}$ meets with the balance equation:

$$p_j=\sum_{i=0}^{\infty}p_ip_{ij} \quad j\ge 0$$

So the average queue length can be solved:

$$\bar{N}=P'(1)=\frac{d}{ds}\left[\frac{(1-\rho)(1-s)A(s)}{A(s)-s}\right]_{s=1} \qquad (3)$$

Using $s=1$ substituting the (3) equation, whose right side is a kind of $\frac{0}{0}$ indefinite equation. When $s\to 1$, using L'Hospital rule twice, average queue length is only decided by ρ and $D[V]$, namely, by serving intensity conditions and square difference of serving distribution, and it is irrelevant to other capabilities of serving distribution.

So the waiting queue length formula:

$$N'=\bar{N}-(1-p_0)=\bar{N}-\rho=\frac{\lambda^2E[V]^2}{2(1-\rho)} \qquad (4)$$

If serving time follows the fixed length distribution, queuing model is M/D/1/∞, it can be concluded that :

$$B(t)=\begin{cases}0, t<a\\ 1, t\ge a\end{cases}$$

$$B^*(s)=\int_0^\infty e^{-st}dB(t)=e^{-as}$$

$$E[V]=a,\quad \mu=\frac{1}{a},\quad \rho=a\lambda,\quad \varphi_b=0$$

So the average queue length:

$$\bar{N}=\rho+\frac{\rho^2}{2(1-\rho)}=\frac{a\lambda}{1-a\lambda}-\frac{(a\lambda)^2}{2(1-a\lambda)} \qquad (5)$$

The waiting queue length:

$$\bar{N}' = \bar{N} - \rho = \frac{(a\lambda)^2}{2(1-a\lambda)} \quad (6)$$

4. STUDYING OF UPSTREAM CELL AVERAGE TIME DELAY

It can be drawn by Little formula:
Average waiting time is:

$$\bar{W} = \frac{\bar{N}'}{\lambda} = \frac{\lambda E[V^2]}{2(1-\rho)} \quad (7)$$

Average staying time:

$$\bar{T} = \frac{\bar{N}}{\lambda} = \frac{1}{\mu} + \frac{\lambda E[V^2]}{1(1-\rho)} \quad (8)$$

When serving time follows fixed length distribution, its queuing model is M/D/1/∞, $E[V] = \alpha$, $\mu = \frac{1}{\alpha}$, $\rho = \alpha\lambda$, $\varphi_b = 0$,

The equation below can be drawn as follows.
Average waiting time:

$$\bar{W} = \frac{\bar{N}'}{\lambda} = \frac{\lambda a^2}{2(1-\lambda a)} \quad (9)$$

Average staying time:

$$\bar{T} = a + \bar{W} = a + \frac{\lambda a^2}{2(1-\lambda a)} \quad (10)$$

The formula (9) and (10) above are the solution of calculating average waiting time and average staying time.

Average staying time is the sum of average waiting time and average serving time, and to real time service and non real time service, waiting time is different.

5. SIMULATION RESULTS

In BPON, upstream cell delay are composed of the following factor: queuing time of arriving cells in ONU; transmission time of upstream queuing information (maximum distance between OLT and ONU is 20km, cell transmission time in the fiber is 100us); processing time of OLT; downstream transmission time of grant; ONU processing time (which is less than 50us[3]); cell upstream transmission time. The simulation results of CD and CDV probability density distribution function are illustrated in Figure 3 and Figure 4, which are concluded by using M/D/1/∞ model on the OPNET software platform. From the figure, CD and CDV can meet the demands] in optical[4][5] network.

6. CONCLUSIONS

Through analyzing and developing of queuing time delay in BPON, the cell time delay in the access network can be reduced. Average waiting time is essential to cell delay in access network, the theoretical algorithm can enhance robustness and improve capability of system, and then raise the parameter of service QoS. Queue length algorithm and formula can provide reference bases to ONU software buffer length designing.

REFERENCES

[1] ITU-T Recommendation G,983,1, *Broadband optical access systems based on Passive Optical Networks[S*], Oct 1998.
[2] Yuke Meng, *Queuing algorithm and its application*, Tongji university publishing house,1989.
[3] Tao Zhang, Ling Li, *Designing of MAC protocol in GPON, Study on Optical communications*, No,5,2004.
[4] ITU-T Recommendation G,982(1996), *Optical access networks to support services up to the ISDN primary rate or equivalent bit rates[S]*.
[5] ITU-T Recommendation I,732, *Types and general characteristics of ATM equipment[S]*, Mar 1996.

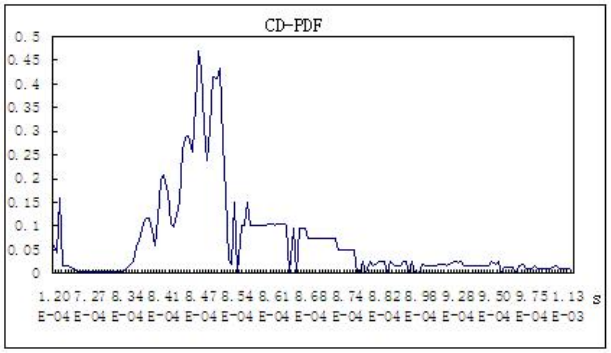


Fig.3. CD probability density

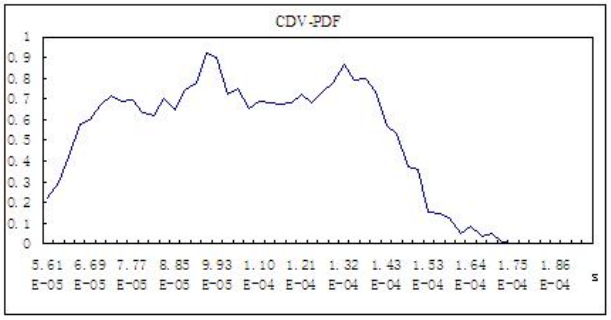


Fig.4. CDV probability density

Hua Liang is a Electrical Engineer, also a teacher of Computer Science and Information Engineering School, Chongqing Technology and Business University. She graduated from Wuhan Transportation University in 1997 with specialty of Industry and Electric automation technology; and got a master' Degree from Wuhan University of Technology in 2005 with specialty of Industrial automation technology. She is a management stuff in Wuhan Iron and Steel Group Corporation from 1997 to 2006. She has acquired Second Class Awards of Hubei Science and Technology Advancement, published 6 Journal papers. Her research interests are in Industrial automation, computer network communication.

Guangxiang Yang is a teacher of Computer Science and Information Engineering School, Chongqing Technology and Business University. He graduated from Wuhan Transportation University in 1997 with specialty of Mechanical and Electrical Engineering technology; and got a master' Degree from Wuhan University of Technology in 2000 with specialty of Mechanical and Electrical Engineering technology; and got a doctor' Degree From Wuhan University of Technology in 2005 with specialty of broadband network access technology. He is a lecturer in Wuhan University of Technology From 2000 to 2006. He has published 15 Journal papers. His research interests are in access network technology, computer testing and controlling.

Research on the Content Distribution Technology of Streaming Media Compromising P2P and CDN

Yunchuan Luo [1], Xiaofeng Hu [1], Yucheng Guo[2], Cunhua Ju [1]
[1] Management Center of National Culture Information Resources Construction Ministry of Culture, China
[2]School of Computer Science and Technology, Wuhan University of Technology, Wuhan, China
Email: scorpionhxf@sohu.com

ABSTRACT

At present, with the development of Internet, the streaming media is increasing so rapidly that it has already become the main format of the Internet information. Comparing with the traditional Web applications such as text and figures, the characters of streaming media are containing large quantity of data and visits which need broader bandwidth and excellent network service. Nevertheless, because of the limitation of the structure of Internet, there are difficulties to apply streaming media in a large scale.

In such conditions, CDN and P2P are developed to resolve the problem of content distribution with respective advantages in different ways, however, there still evident shortages for the limitation of the computing models of CDN and P2P. In this paper, a new streaming media content distribution model is discussed depending on the compromising of CDN and P2P.

Keywords: P2P, CDN, Compromising

1. INTRODUCTIONS TO THE TRADITIONAL CDN AND P2P

1.1 Introduction CDN

The full name of CDN is Content Delivery Network. In this way, the content can be delivered from the core to the nearest end point of the network, where the best service is provided by adding a layer of new network framework and using the passing intelligent tactics, and the users can access to the needed information nearby. By this means, the crowding of the Internet is released and the response time of the website is reduced. From technical aspect, CDN resolves the problem that the visit of the user is responded too slowly, which is caused by the narrow bandwidth, numerous visitors, as well as the uneven distribution of the network stations.

However, CDN still belongs to the Client/Server computing model. Although it can distribute the functions and services in the network, which will promote the delivery of the content of streaming media in a certain degree and improve the service as well, the service extending ability is decided by repeated arrangement of the delivery nodes with high cost and continuous investment because its core is depending on the framework of C/S. Further more, because users' visits are random and unexpected, without elastic extending ability CDN can not promote the efficiency of the system basically.

1.2 Introduction to P2P

The full name of P2P is Peer to Peer, that means transmitting equally from point to point. P2P integrates the single user into network. In this way, the bandwidth can be shared and the information is processed in together. Different from the traditional C/S model, all clients have the service function. Using the framework of P2P, the computing resources and the bandwidth of the common computing apparatuses are used efficiently, and the computing tasks and memorized data are delivered to every peer. As the result, high performance computing, strengthened I/O ability, broader bandwidth as well as enormous storage can be realized. As the same time, because of the characters of P2P, the advantages are significant when synchronous services of the system are demanded in a large scale. The system has the ability of dynamic extending, and it can provide efficient and reliable service with low delivery cost.

Nevertheless, shortages still exist in the application of single client P2P. Firstly, P2P system is difficult to be controlled and not manageable inborn, so there is the problem of utilizable ability. P2P is reliable from the aspect of the whole system, but focusing on the individual content or task, the system is not satisfied. Every peer is random and can quit the system, as well as the content for exchanging can be deleted and the sharing of it can also be terminated at all times. Further more, using the traditional technology, the best logical links are chosen as the channels for data exchanging automatically, but the condition of the practical physical links are ignored. The real framework of the IP network of telecom has not been considered which leads to problems harming the benefits of the telecom merchants such as the block and streaming storm of the back-bone network. All these hinder the traditional client terminal P2P developing into the technical platform in the level of telecom.

2. THE PRACTICABILITY OF THE COMPROMISING OF P2P AND CDN

P2P is an elastic system can be extended at anytime with high service efficiency, its weak concentrates on the management of content copyright and users, the insurance of Qos service as well as the sequence of the data stream. On the contrary, CDN technology has the advantage in the ensured service and manageable content and client, but because of its inflexible character, the efficiency of the system is difficult to be promoted and large scale service is hardly to be realized with low cost.

From above, we can learn that, as two main technologies of content distributing, both CDN and P2P has superiorities in their own field. Further more, there are complementarities in the difference between their computing models. If we can compromising the extending ability of P2P with the reliable and manageable character of CDN, a streaming media delivery platform can be constructed which will fulfills the responsibility of the content application in the level of telecom.

3. THE COMPROMISING OF P2P AND CDN

Considering the research on P2P and CDN, a new model is conceived which adopt traditional CDN as the upper

framework and P2P as the lower layer to realize the content distributing. Using the traditional CDN technology, the content of streaming media is pushed from the core to the end of the network and cached in the service peer. And then, using P2P technology, the transmitting must be limited within the service of local peer. If the local peer does not have the content needed by the user, it will ask the central server for it, and then deliver the content to the local client after fetching it. This model combines the respective characters of traditional P2P and CDN. On the one hand, the content is pushed to the peer nearest to the user depending on the ensured service of CDN; on the other hand, the service ability is promoted through the advantage of extending of P2P.

However, combining P2P with CDN in this way just uses the outside characters of themselves, the nature of these two technologies has not been touched, and the frameworks of them has not been compromised yet. Just their serving methods are added up. Only when the superiorities of P2P and CDN are utilized completely, can the compromising of them be realized, that means not only the advantages in service should be utilized, but also their shortages should be remedied by the superiorities of the other side. At last, after composition and unification, an optimized platform of streaming media content delivery is built up which compromises CDN and P2P.

The CDN can be optimized and modified by P2P. In the traditional CDN, the data links between the core and the end service point need quite a lot of investment, but utilizing rate of the resources and bandwidth is not high. Further more, the unimpeded transmission of the links across ISP can not be ensured. Facing this problem, the node apparatus of CDN should be organized in the way of P2P, using the list service and multi-peer transmitting function of it, the content of the different node equipments of CDN can be exchanged and duplicated. Then content delivery ability of CDN is improved for in this way, the transmitting of the content from the core to the end is accelerated and the redundancy of the system is improved.

Absorbing the advantage of CDN, using the management system of it, increasing the position of the super nodes, a framework can be constructed in which CDN is the reliable content core and P2P is the extending mechanism. In such way, the content and users can be well managed and the streaming load of the network will be in order.

All in all, the compromising of CDN and P2P does not mean the simple composition of them. On the one hand, adopting P2P to optimize the core layer of CDN and re-organize the original framework and service point of it; on the other hand, using the technology of CDN to improve the function of control and management of P2P network.

After completed compromising, infiltration and modification, a unified optimized content distribution platform (the upper layer is CDN with improved delivery ability after being modified by P2P, and the lower layer is P2P with strengthened function of control and management) compromising CDN and P2P is formed.

4. THE ADVANTAGE OF THE COMPROMISING MODEL

The streaming media content distribution platform compromising P2P and CDN has the advantages as following.

First, the pressure on the data resources of the central peer is released greatly. In the traditional CDN, if any point wants to acquire the data of the resources of the central point, it must visit the server of the data resources in direct, which cause that the pressure on the data resources is too extensive and waste too much bandwidth as well as affecting the stability of the link between the center and the end point. Instead, data in the CDN which has been re-organized in the way of P2P can be shared and cached, so that the pressure on the central data resources is released in a great degree.

Second, the reliability of the system is enhanced by the multiple back-ups of the data of central data resources. Multi-peer back up is the result of that different service peers duplicated the data of the central resources, which strengthens the redundancy of the CDN system as well as the ability of the self repairing of the service, so that the stability of the whole system is improved.

Third, flexible service is realized by adding service nodes. The data is shared and cached in the way of P2P, which releases a lot of nodes to provide service that is much more flexible and intelligent. For example, using streaming media VOD, the nodes in neighborhood can cache different streaming media data in a certain sequence respectively. If the user of node A requests the content cached in node B, the data will be exchanged between the two nodes, at last the user will acquire the content from node A.

Fourth, the efficiency of the service is promoted by strengthening the extending ability of the system. Using P2P technology to deliver the content in the lower layer improve the extending ability of the system significantly, a elastic system can deal with the bursting out of the unexpected visits, which will maintain the high service efficiency.

The streaming load in disorder can be avoided by enhancing the management of the network. Because the range of P2P is strictly limited in a certain service area of a specific end service peer, many problems such as block of back-bone network and the disorder of the streaming load can be resolved, which used to be caused by the transmission across regions and ISP of P2P. Thus the network is much more manageable and the good service is ensured. Further more, both the users and the streaming load can be supervised through the client terminal.

5. CONCLUSIONS

After compromising P2P with CDN, the shortages of the two technologies can be remedied by the advantages of the other side, and the original framework is modified. In addition, the extending ability of P2P and the reliability and manageable ability of CDN are integrated perfectly. All these provide an opportunity to construct a super content distribution platform which can support the delivery and the application of the content in the level of telecom.

REFERENCES

1) “A CDN-P2P Hybrid Architecture for Cost-Effective Streaming Media Distribution”, Author: ngyan xu,Sunil Suresh Kulkarni,Catherine Rosenberg,Heung-keung chai.
2) “A Hybrid Architecture for Cost-Effective On-Demand Media Streaming”, Author:M. Hefeeda，Bharat K. Bhargava，David K. Y. Yau.

Yunchuan Luo was born in 1974, He works in the Management Center of National Culture Information Resources Construction of Ministry of Culture. His main research interests are in the area of business intelligence, data transforming and processing, distributed parallel processing, server cluster design and implementation

Xiaofeng Hu was born in 1980, He works in the Management Center of National Culture Information Resources Construction of Ministry of Culture. His main research interests are in the area of distributed parallel processing, server cluster design and implementation, graphic and image processing.

Cunhua Ju was born in 1979, she works in the Management Center of National Culture Information Resources Construction of Ministry of Culture. Her main research interests are in the area of management and service of digital resources, data Warehouse, data excavation.

The Load of Kautz Networks with Shortest Paths *

Li Sun [1], Changle Zhou [1] and Jianguo Qian [2]
[1.] Computer and Information Engineering College, Xiamen University, Xiamen,Fujian Province 361005, P.R. China
[2.]School of Mathematical Sciences, Xiamen University, Xiamen,Fujian Province 361005, P.R. China
Email:sun8819030@sohu.com

ABSTRACT

Under the all-to-all communication mode and shortest path scheme, this note shows that the load of an edge in a Kautz network $K(d, k)$ is upper bounded by $1 + 2d + 3d^2 + \cdots + kd^{k-1}$. The sufficient-necessary condition for an edge to reach this bound is also given. This result implies that if $d \geq 2+\sqrt{k-1}$ then the load of the Kautz network equals $l(K(d, k)) = 1 + 2d + 3d^2 + \cdots + kd^{k-1}$.

Keywords: WDM Networks, Shortest Path Routing, Network Loads

1. INTRODUCTION

With the development of optical fiber techniques, more and more optical fiber techniques such as Wavelength Division Multiplexing (WDM) are introduced into multiprocessor interconnection and computer networks interconnection. Single hop network is optical networks in which no Wavelength converter is used [1]. In single-hop networks two end-nodes must communicate with one another in one hop, that is, the connection between a pair of nodes should use the same wavelength throughout the route of the light-path. In WDM scheme, frequency multiplexing in the optic domain is used where several communication channels operate at different carrier frequency on a single fiber subject to the constraint that two different light-path sharing a fiber must use separate channels. In all-to-all communication mode, every node sends messages to each of the others through light-path between them. The number of light-path passing through a fiber is called the load of this fiber and the maximum load of the fibers in the network N is defined as the load of N [2]. While the ability of a fiber to bear light-path is limited and when the scale of the network is extended, the load of the network will increase and may be more than the fiber can bear. So how to lower the load of a fiber and save the wavelength resource is a key problem for an all-optical network.

An optical network is convenient to be modeled as a directed graph G = (V, E)(with V as the node set and E as the edge set). The Kautz digraph is frequently used in modeling networks topology because it is regular, smaller in diameter and better fault tolerance. The other properties of Kautz networks have been studied to evaluate their suitability as topology for optical networks. For example, Kautz networks has better performance such as for given degree of each node and a given diameter of the network; it supports more nodes than other topologies, it also has better performance in terms of queuing delay in multi-hop networks[3]. The fault tolerant routing ability of Kautz networks is studied in literature [4].

It is known that there is only one shortest path between any two nodes in Kautz digraph, that is, the shortest path routing scheme is determined once the parameter of Kautz digraph is given. The shortest path routing algorithm was proposed in literature [3]. By all-to-all communication mode in single hop optical network, there is a light-path between any two nodes, the message can be transmitted in the light--path by one wavelength.

In this paper, we will focus on the all-to-all communication mode and shortest path scheme of the Kautz network. We show that the load of an edge (denoted by $l(e)$) in a Kautz network $K(d, k)$ is upper bounded by $1 + 2d + 3d^2 + \cdots + kd^{k-1}$. The sufficient-necessary condition for an edge to reach this bound is also given. This result implies that if $d \geq 2+\sqrt{k-1}$ then the load of the network equals $l(K(d, k)) = 1 + 2d + 3d^2 + \cdots + kd^{k-1}$.

2. MAIN RESULTS

For two vertices u and v of a graph G, we denote by (u, v) the directed edge with direction from u to v. Given two positive integers d and k, the Kautz digraph $K(d, k)$ [4] is defined to be a regular digraph whose node set consists of all strings $a_1 a_2 \cdots a_k$ of length k, where $a_i \in \{0,1,2,\cdots,d\}$, $i=1,2,\cdots, k$, $a_i \neq a_{i+1}$ for each $i \in \{1, 2, \cdots, k-1\}$ (i.e., any two successive symbols in the string are distinct); and two nodes (strings) u and v have an directed edge from u to v provided they have the form $u = a_1 a_2 \cdots a_k$ and $v = a_2 \cdots a_k a_{k+1}$. One can see easily that $K(d, k)$ have $d^k + d^{k-1}$ nodes with degree d and diameter k. As an example, $K(2, 3)$ is as shown in figure 1.

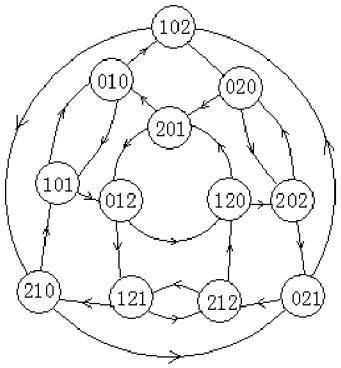


Fig.1. The Kautz network K(2, 3).

When we say that a string $a_1 a_2 \cdots a_k$ is equal to $a'_1 a'_2 \cdots a'_{k'}$, denote by $a_1 a_2 \cdots a_k = a'_1 a'_2 \cdots a'_{k'}$, we always mean that $k = k'$ and $a_i = a'_i$ for all $i = 1, 2, \cdots, k$. For two (or more) strings $w = a_1 a_2 \cdots a_k$, $w' = a'_1 a'_2 \cdots a'_{k'}$, we denote by ww' the connection of w and w', i.e., $ww' = a_1 a_2 \cdots a_k a'_1 a'_2 \cdots a'_{k'}$.

Theorem 1. For any edge $e = (a_1 a_2 \cdots a_k, a_2 \cdots a_k a_{k+1})$ of $K(d, k)$,

$$l(e) \leq l_{\max} = 1 + 2d + 3d^2 + \cdots + kd^{k-1},$$

and the equality holds if and only if non of the following three cases holds.

1). There exist $i, j \in \{1, 2, \cdots, k\}$, $i \geq j+1$, such that a_1

* Research supported by NSFC(10671162) and the Program of 985 Innovation Engineering on Information in Xiamen University (2004-2007)

$a_2 \cdots a_j = a_i a_{i+1} \cdots a_{i+j-1}$;

2). There exist $i, j \in \{1,2, \cdots, k\}$, $j \le i+k-j$, such that $a_i a_{i+1} \cdots a_j = a_{i+k-j+1} a_{i+k-j+2} \cdots a_{k+1}$;

3). There exist $i, j \in \{1, 2, \cdots, k\}$, $2j - i - 1 \le k$, such that $a_i a_{i+1} \cdots a_{j-1} = a_j a_{j+1} \cdots a_{2j-i-1}$.

Proof Let $e = (a_1 a_2 \cdots a_k, a_2 a_3 \cdots a_{k+1})$ be an arbitrary edge of $K(d, k)$. Then the initial node u and the terminal node v of a path $P : u \rightarrow v$ passing through e has the form:

$$u = b_1 \cdots b_{k-s} a_1 a_2 \cdots a_s$$

and $$v = a_t a_{t+1} \cdots a_{k+1} c_1 \cdots c_{t-2}, \quad (1)$$

where $s, t \in \{1, 2, \cdots, k\}$, $t \le s + 1$. Recall that any two successive symbols in the string are distinct and notice that the number of all the symbols b_i and c_j equals $(k - s) + (t - 2)$. This implies that, when s and t are fixed, then the number of all the possible paths is no more than $d^{(k-s)+(t-2)}$. Therefore, when $s - t$ is fixed, say $s - t \ge -1$, the number of the possible such paths is no more than

$$((k - s) + (t - 2) + 1) \times d^{(k-s)+(t-2)}$$

On the hand, we notice that $-1 \le s - t \le k - 2$. Thus, the number of all the possible paths passing through e is no more than

$$1 + 2d + 3d^2 + \cdots + kd^{k-1},$$

as desired.

Now suppose that non of the three cases mentioned in the theorem holds. From the above discussion, to prove $l(e) = l_{\max}$, we need only to prove that the path P with initial node $u = b_1 \cdots b_{k-s} a_1 a_2 \cdots a_s$ and terminal node $v = a_t a_{t+1} \cdots a_{k+1} c_1 c_2 \cdots c_{t-2}$ must pass through e for any $b_1, \cdots, b_{k-s}, c_1 c_2 \cdots c_{t-2} \in \{1, 2, \cdots, d\}$(with the restriction that any two successive symbols in the string are distinct). Since from u we can reach v by $(k - s) + (t - 2)$ steps, the distance $d(u, v)$ from u to v is at most $(k - s) + (t - 2)$. Furthermore, it is clear that if $d(u, v) = (k - s) + (t - 2)$ then P must pass through e. Now assume that

$\rho = d(u, v) < (k - s) + (t - 2)$.

Case 1. $\rho < k - s$ and $k - \rho \le (k + 1) - t + 1$.

This case implies that

$$b_{\rho+1} \cdots b_{k-s} a_1 a_2 \cdots a_s = a_t a_{t+1} \cdots a_{t+k-\rho}.$$

That is, $a_1 a_2 \cdots a_s = a_{t+(k-s)-\rho+1} a_{t+(k-s)-\rho+2} \cdots a_{t+k-\rho}$, which contradicts the fact that e does not meet the condition 1).

Case 2. $\rho < k - s$ and $k - \rho > (k + 1) - t + 1$.

Let $w = (k - \rho) - ((k + 1) - t + 1)$. Then we have

$$b_{\rho+1} \cdots b_{k-s} a_1 a_2 \cdots a_s = a_t a_{t+1} \cdots a_{k+1} c_1 \cdots c_w$$

This implies that

$$a_1 a_2 \cdots a_{s-w} = a_{k+w-s+2} a_{k+w-s+3} \cdots a_{k+1},$$

which contradicts the fact that e does not meet the condition 1) and 2).

Case 3. $\rho \ge k - s$ and $k - \rho \le (k + 1) - t + 1$.

This case implies that

$$a_{\rho-(k-s)+1} a_{\rho-(k-s)+2} \cdots a_s = a_t a_{t+1} \cdots a_{t+k-\rho-1}$$

and therefore,

$$a_{\rho-(k-s)+1} a_{\rho-(k-s)+2} \cdots a_{t-1} = a_t a_{t+1} \cdots a_{2t+k-\rho-2}.$$

This contradicts the fact that e does not meet the condition 3).

Case 4. $\rho \ge k - s$ and $k - \rho > (k + 1) - t + 1$.

Let $w = (k - \rho) - ((k + 1) - t + 1)$. Then we have

$$a_{\rho-(k-s)+1} a_{\rho-(k-s)+2} \cdots a_s = a_t a_{t+1} \cdots a_{k+1} c_1 \cdots c_w.$$

This implies that

$$a_{\rho-(k-s)+1} a_{\rho-(k-s)+2} \cdots a_{s-w} = a_t a_{t+1} \cdots a_{k+1},$$

again a contradiction to the fact that e does not meet the condition 2).

Conversely, from the above discussion, we can also see that if one of the three cases holds, then the number of the paths pass through e will not reach the upper bound $l_{\max}$. For an example, if there exist $i, j \in \{1, 2, \cdots, k\}$, $i \ge j+1$, such that $a_1 a_2 \cdots a_j = a_i a_{i+1} \cdots a_{i+j-1}$, then the length of the path P from the node $b_1 \cdots b_{k-j} a_1 a_2 \cdots a_j$ to $a_{j+1} a_{j+2} \cdots a_{k+1} c_1 \cdots c_{j-1}$ is at most $k - i$ if we choose $b_{k-i+2} = a_{j+1}$, $b_{k-i+3} = a_{j+2}$, $\cdots$, $b_{k-j} = a_{i-1}$. Notice that

$(k - j) + (j - 1) = k - 1 > k - i$. This implies that the number of the total paths which pass through e with $s = j$ and $t = i$ (here s and t is as defined above) will not reach the upper bound $d^{(k-s)+(t-2)}$ and therefore,

$l(e) < l_{\max}$. The discussion for other two cases are analogous. This completes our proof.

Corollary 1. If $d \ge 2 + \sqrt{k-1}$ then

$$l(K(d, k)) = 1 + 2d + 3d^2 + \cdots + kd^{k-1}.$$

Proof. We need only to find out an edge e of $K(d, k)$ which does not satisfy any one of the three conditions of Theorem 1. Let the strings

$$w = 1213 \cdots 1(d-1)2324 \cdots 2(d-1) \cdots (d-2)(d-1)$$

(e.g., when d = 5, we have w = 12131415232425343545) and $w^* = w1w^{-1}$, where w^{-1} is the inverse of w(e.g., 1236547^{-1} = 7456321). It can be verified that w^* is a string of length $2 \times (1+2+\cdots+(d-1))+1 = d(d-1)+1$ and furthermore, it does not satisfy any one of the three conditions of Theorem 1. For convenience, we write $w1w^* = w_1 w_2 \cdots w_{d(d-1)+1}$.

Since $d \ge 2 + \sqrt{k-1}$, we have $k < d(d - 1) + 1$. This means that e does not satisfy any one of the three conditions of Theorem 1 if we choose

$$e = (0 w_1 w_2 \cdots w_{k-1}, w_2 w_3 \cdots w_k d),$$

which completes our proof.

REFERENCES

[1] B. Mukherjee, "WDM-based local light wave networks Part 1: single-hop system," *IEEE Network,* 6(3), 1992, pp.12-26.

[2] Xiaohua Jia, Xiao-dong Hu, Ding-zhu Du, *Multiwavelength Optical Networks*, Kluwer Academic Publishers,2002.

[3] Geetha Panchapakesan, Abhijit Sengupta "On a Lightwave Network Topology Using Kautz Digraphs," *IEEE Transactions on Computers,*1999, Vol. 48, pp.11311138.

[4] Wei-kuo Chiang, Rong-jake Chen; "Distributed fault-tolerant routing in Kautz networks," *Journal of parallel and distributed computing,* 1994, vol.20, pp.99-106.

Research and Implementation on VLAN-IP Technology*

Wei Xiong, Chuanqing Cheng
Computer Science Departement
Wuhan University of Science and Engineering
Wuhan,China
Email: case100101@163.com

ABSTRACT

With the change of network dimensions, Ethernet technology has developed from LAN to campus network, so the Layer-2 switch has developed to multi-layer switch. The appearance of layer-3 or upper layer switch ,can solve the problems of low forward rate, high delay of traffic that needs to cross networks. This paper introduces the principle, character and implementation in detail. From this ,we can see that the point of "one route ,many times to layer-2 forward" is error. Layer-3 switch replace the software look up technology with the high speed ASIC forwarding.VLAN-IP technology is discussed in detail in the paper.

Key words: IP, Layer-3 Switch, VLAN, QoS

1. INTRODUCTION

With the change of network dimensions, Ethernet technology has developed from LAN to campus network, so the Layer-2 switch has developed to multi-layer switch.

The appearance of layer-3 or upper layer switch ,can solve the problems of low forward rate, high delay of traffic that needs to cross networks.

There are some inaccuracies if Layer-3 switch principle, This paper will introduces principle, character and implementation of the Layer-2 switch,Layer-3 switch, and multi-layer switch based on flow classification

2. VLAN

To understand VLANs, it is first necessary to have an understanding of LANs. A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Communications with devices on other LAN segments requires the use of a router. LAN environment connected by routers. Note that the router interface for each LAN is included as part of the LAN and broadcast domain.

As networks expand, more routers are needed to separate users into broadcast and collision domains and provide connectivity to other LANs.

Virtual LANs (VLANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment. VLANs provide a number of benefits over the network.

* This work is supported by Hubei Province Natural Science Foundation under Grant 2006ABA296

When address mating is done ,chip compares MAC+VID, only when the two are both matched, the packet can forward successfully.

In Layer-2 switch, VLAN only means isolation of broadcast domain and is not involving gateway, which is done by upper layer devices.

In layer 3 switch, VLAN is used to partition layer 2 broadcast domain and VLAN-IP architecture is used to partition IP subnet, which can unify the layer 2 broadcast domain and layer3 IP subnet.

3. LAYER-3 SWITCH

3.1 Subnet and Gateway

Layer-3 switch is network switch, which means packet forwarding is done by IP address of packets.

The most important concept of network layer is IP subnet and gateway.

IP is a protocol to mark host address in the network layer when packet is being transmitted. IP address is signed by four groups of 8 bits .(just like 192.168.2.1).It is composed of two parts. The former parts is network address, the latter is host address. The subnet is to mark how many bits of the IP address is belong to network address.

When looking for address,the subnet is used to judge the destination IP address of packet is local or must be routed.
Gateway is router, which can used to forward packet between two subnets.

Simplify to said ,to distinguish whether the two hosts is in the same subnet, can bit AND there IP address with the subnet mask, if the result is same ,the two is in the same subnet. When two hosts in the same subnet ,the communication is only on data link layer, even if the communication is IP communication. But communication of the hosts in different subnet need network layer device-router or Layer-3 switch.

3.2 VLAN –IP Architecture

Each network vlan has the following feature:

- Each vlan has a related mac address ,and can be set an ipv4 network address and a mask.
- Each vlan which is set a ipv4 network address/mask can be a network interface, which is bound with the OS protocol stack. The subnet of this vlan can communication to the end-station inside via the network interface.
- The ipv4 address /mask of the vlan is set by the host as the default gateway.
- The vlan can isolate layer2 broadcast domain, the broadcast packets and the unknown packets will flood within the vlan but not to other.

- According to the practical need ,the end stations in different vlans can be set to communication each other or not
- Each vlan which is set a ipv4 network address/mask is bound with OS protocol stack as a independent device in the low layer driver, and responsible for process and reply the communication with the ip.

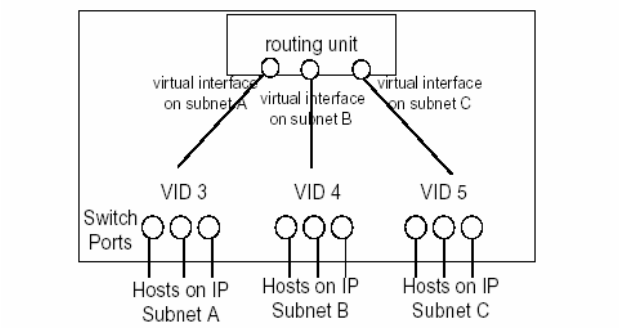


Fig.1. VLAN and subnet

3.3 Flow of IP Forward

ARP, is address parse protocol, which is responsible for parsing the according MAC address of IP address. ARP is very important in IP communication. The layer-3 switch is based on ARP. We take three hosts as example, to introduce the IP forward flow in the same subnet and different subnet. We will take ping protocol as example.
The three hosts are configured as Table 1.

Table 1 THREE HOSTS

	A	B	C
IP address	1.1.1.1	1.1.1.2	2.1.1.1
Subnet mask	255.0.0.0	255.0.0.0	255.0.0.0
gateway	1.1.1.254	1.1.1.254	2.1.1.254
MAC address	000000000 00a	00000000000 b	0000000 0000c
VLAN	VLAN1	VLAN1	VLAN2

(1) A communicate with B

- A takes its IP address bit AND with subnet mask, and gets the network ID :1.0.0.0
- B takes its IP address bit AND with subnet mask, and gets the network ID :1.0.0.0,which is same with A.
- Because the destination host is in the same subnet with itself ,A send ARP packet ,the tar get IP is 1.1.1.2.
- Host B receives the ARP request from A, records the IP-MAC information of A, and send ARP reply packet to A.
- Host A receives the ARP reply ,records the IP-MAC information of B, sends the ICMP echo packet ,in which the destination MAC is 0000000000000b

Now the switch has the entry of MAC 0000000000b,the matching is successful, and the destination port is in the same VLAN with the source port ,so ICMP echo can forward to host B via layer-2 switch.

The ICMP reply sent back by Host B forward to host A as the same .

From the example, it is obvious that the gateway of host A and host B,1.1.1.254, is not involving the communication process. The packet forward is according to MAC address ,which is a typical data link layer switch.

(2) A communicate with C

The communication of A and C will use the MAC of gateway, which is the MAC address of VLAN. The gateway IP address is the IP address of VLAN. So the VLAN is set like Table 2.

Table 2 VLAN IP/MAC

	VLAN1	VLAN2
IP address	1.1.1.254	2.1.1.254
MAC address	000000000001	000000000002

- A takes its IP address bit AND with the subnet mask, gets the network ID:1.0.0.0
- C takes its IP address bit AND with the subnet mask, gets the network ID 2.0.0.0
- Because the destination host is in the different subnet with itself, host A sends ARP packet, whose target IP address is 1.1.1.254.Gateway must take part in the forwarding of different subnet.
- Gateway A receives the ARP request of host A, records the IP address and MAC address, send ARP reply packet.
- Host A receives the ARP reply packet records the IP address and MAC address of gateway(VLAN1),sends ICMP echo packet, whose destination MAC is MAC of gateway and destination IP is the IP of host C.

It is obvious that only IP address of host C can be get from the ICMP echo packet. So the forwarding must be according to IP

4. IMPLEMENTATION OF LAYER-3 SWITCH

From section 3,we know the packet in different subnet must forward according to network layer information. So there should be a IP forward table just like FDB, from which the relation of IP and port can be get. But IP forward table is formed by software not as FDB by hardware.

The key problem is to distinguish which packets must forward by FDB, and others by IP forward table From the two examples of section 3,we know ,the packet via layer-2 have no information of gateway, and the packet via layer-3 regards the gateway's MAC address as its destination MAC address. The current switch ASIC supply the function ,can decided a packet whether to send to layer-3 module when matching the MAC address by a bit configuration.

So the key technologies of implementing layer-3 switch is :

(1) VLAN binds to protocol layer and driver

VLAN can be set IP address/mask/MAC address and binds to protocol layer. For the host in the subnet, the default gateway can be set to be the IP addess/mask. Then the VLAN binds to the driver, as a device to do sending and receiving of packets and processing the communication with the IP address.

This step is to assure the communication of host and gateway. Gateway can process ARP protocol and etc.

(2) write the MAC address of VLAN to fdb, and set the L3 bit
This step is to send the packet which need gateway to take part in to ROUTE module, to be forwarded according to IP address.
(3) CPU process the ARP send/received, write some IP address and the corresponding port to IP forward table.

From the examples of seciton3, we know the ARP with gateway is the foundation of layer-3 switch. Just we can get the information of ARP with gateway, we can get the host IP address information. Although there is no port information in ARP packet, FDB supply the information. So it is easy to get relation of IP address and port to set a IP forwarding table.
It is different from layer-2 switch, Layer 3 switch comes true by software-hardware cooperation but layer-2 switch is a pure hardware operation.

When IP forward table is formed ,the forwarding is by ASIC with high speed. The forwarding performance between subnet improved greatly.

5. CONCLUSIONS

This paper introduces the principle, character and implementation in detail. From this ,we can see that the point of “one route ,many times to layer-2 forward” is error. Layer-3 switch replace the software look up technology with the high speed ASIC forwarding. Multi-layer switch is based on flow classification technology and QOS.

REFERENCES

[1] *COMERDE.Internetworking With TCP IP* Vol1.I[M]. Beijing:Prentice-Hall,2000.
[2] Xie Xizen, *Compute Network*, Beijing, Electronics Press, 1999.
[3] LISTANTIM, “Architectural and Technological Issues for Future Optical Internet Network[J],” *IEEE Comm Magazine*, 2000,38(9),pp.82-92.
[4] He Xiaoming, “Analysis of layer-3 switch,” *Chinese data communication*, 2003.
[5] G.R.McClain, “Hand Book of Networking and Connectivity,” AP Professional, Boston, MA,1994.
[6] J.Gong and P.Srinagesh, “An Economic Analysis of Network Architecture,” *IEEE Network*, vol.10,no.2,March/April 1996,pp.18-21.

Wei Xiong (1983-) a student of Wuhan University of Science and Engineering. The research filed is computer network and communication network.

Distributed System Architectures

Functional Parallel Programming Environment For Multicore Computers and Clusters *

S.E. Bazhanov[1], V.P. Kutepov[2], M.M. Vorontsov[3]
Applied Mathematics Department, Moscow Power Engineering Institute (Technical University)
ul. Krasnokazarmennaya 14, Moscow, 111250 Russia
Email: [1]s_bazhanov@mail.ru, [2]KutepovVP@mpei.ru, [3]mikew@avtobank.ru

ABSTRACT

In the paper, a functional parallel programming system for clusters and multicore computers is discussed. It includes a language of parallel programming, program development tools, and tools for controlling parallel execution on the computer system. Central part of the system is original parallel compositional functional programming language FPTL (Functional Parallel Typified Language).

Keywords: Parallel Programming, Cluster, Multicore Computer, Functional Programming Language, Parallel Software Tools.

1. INTRODUCTION

Recent tremendous progress in the development of parallel systems, the possibility of the creation of clusters from personal computers using standard network communications, wide expansion of multicore computers and, finally, appearance of new scientific and engineering problems that require high-performance systems for their solving make the researchers return to the problem of the development of efficient systems for parallel programming and management of parallel processes.

In this paper, we describe a functional programming system for clusters, which was developed in the framework of a project headed by Professor Kutepov at the applied mathematics department of the Moscow Power Engineering Institute. In the course of the project realization, we took into account both our own experience of the development of the functional programming systems and the experience of the creation of similar systems accumulated by foreign researchers.

Functional programming system concerned consists of three components: parallel programming language, tools for controlling parallel execution of program on the computing system and program development tools.

System's central part is the original compositional functional parallel programming language FPTL (Functional Parallel Typified Language). The most remarkable features of the language are:
– functions are specificated in terms of schemes;
– FPTL – multilanguage tool, one can import functions from programs in other programming languages;
– the FPTL is a strictly typified language with a static type check of programs;
– the FPTL provides a module specification of a program;
– the model of execution of FPTL-program is inherently parallel.

* This project is supported by the Russian Foundation for Basic Research (No. 06-01-00817).

The paper is organized as follows. In Section 2, a brief theoretical introduction to the language is given. Section 3 discusses basic principles of the construction of the programming environment for the functional program development, its main blocks, models underlying them, and specific features of their implementation.

2. FUNCTIONAL PARALLEL PROGRAMMING LANGUAGE FPTL

2.1 Function Definition

Data and, generally, the partial functions defined on the data are the main semantic FPTL objects.

Following [2, 4-8], we consider the functions to be the (m, n)-ary, m≥0, n≥0, typified correspondence between the data sets; the (m,n)-ary function f(m,n) is the one-valued correspondence, partial in the general case, from $D_1 \times D_2 \times \dots D_m$ to $D'_1 \times D'_2 \times \dots D'_n$ of the type $t_1 \times t_2 \times \dots t_m \to t'_1 \times t'_2 \times \dots t'_n$, where ti and t'_j, i = 1, 2, …, m, and j = 1, 2, …, n are the types whose values are the nonempty sets Di and D'_j respectively. Di and D'_j are supposed to include a computed indefinite value denoted as ω. Thus, the arguments and values of the (m,n)-ary function are the data tuples of the length m and n. The condition $\alpha\lambda = \lambda\alpha = \alpha$ is fulfilled for any tuple α, where λ is the tuple of zero length.
The function f(m,n) is uniquely represented by its graph $\{(\alpha, \beta) \mid f(m, n)(\alpha) = \beta\}$, where α and β are the data tuples. In what follows, the tuples are represented as a concatenation of their elements without separators: α, β, γ, … designate arbitrary tuples.

In the general case, data and functions in FPTL are defined by systems of functional or relational equations in given signatures treated as operators of the minimum fixed point or the minimum solution of systems of equations under consideration. We call the parameterized functions and data types functionals and relationals, respectively.

In theory, the set of functions in FPTL represents an inductive class of functions obtained by closing the set of operations of the composition of functions O over the given set of basis functions F. The pair <O, F>can be treated as a free functional algebra.

FPTL uses four simple operations of the composition of functions that are in a sense a reduction of conventional mathematical ways of defining a function by the case analysis and substitution of other functions for arguments of the known one. The Herbrand-Godel model of defining computable functions and the language of recursive functions are the prototypes of the approach we use to define the computable functions. The fundamental difference is that the general case of constructing an arbitrary computable function over abstract

data types is proposed in FPTL instead of the unified data structure, viz., the natural scale and the model of computable functions specified on it. The four operations of composition of functions considered in what follows, the operator of function definition by systems of functional equations, the set of functions–constructors "extracted" from the definition of the abstract data type, and the functions–destructors reciprocal to them form the universal signature that allows us to express any computable function over the considered data type [2, 8].

We describe the operation of composition using the following designations: f(m,n) is the (m,n)-ary function and f(m,n)(a) is the result of applying it to the tuple a, f1 and f2 are known functions, f is the definable function, and is the equality sign according to the definition.

1. The operation of sequential composition (•)

$$f^{(m,n)} \equiv \left(f_1^{(m,k)} \bullet f_2^{(k,n)}\right) =$$

$$= \left\{(\alpha,\beta)\,\middle|\, \exists\gamma(\alpha,\gamma) \in f_1^{(m,k)} \wedge (\gamma,\beta) \in f_2^{(k,n)}\right\};$$

$$f^{(m,n)}(\alpha) \equiv f_2^{(k,n)}\left(f_1^{(m,k)}(\alpha)\right).$$

2. The operation of concatenation (∗)

$$f^{(m,n_1+n_2)} \equiv \left(f_1^{(m,n_1)} * f_2^{(m,n_2)}\right) =$$

$$= \left\{(\alpha,\beta_1\beta_2)\,\middle|\, (\alpha,\beta_1) \in f_1^{(m,n_1)} \wedge (\alpha,\beta_2) \in f_2^{(m,n_2)}\right\};$$

$$f^{(m,n_1+n_2)}(\alpha) \equiv f_1^{(m,n_1)}(\alpha) f_2^{(m,n_2)}(\alpha).$$

3. The operation of conditional composition (→)

$$f^{(m,n)} \equiv \left(f_1^{(m,n_1)} \to f_2^{(m,n)}\right) =$$

$$\left\{(\alpha,\beta)\,\middle|\, (\alpha,\beta) \in f_2^{(m,n)} \wedge \exists\gamma\left((\alpha,\gamma) \in f_1^{(m,n_1)}\right)\right\};$$

$f^{(m,n)}(\alpha) \equiv f_2^{(m,n)}(\alpha)$ if the value $f_1^{(m,n)}(\alpha)$ is defined; if $f_1^{(m,n)}(\alpha) = \omega$ or it is computed endlessly, then the value $f^{(m,n)}(\alpha)$ is considered indefinite. For this conditional construction to be in agreement with the conventional one, when is the propositional function possessing two values "true" and "false," we assign the "false" value to be identical to ω.

4. The operation of the union of graphs of functions (⊕):

$$f^{(m,n)} \equiv \left(f_1^{(m,n)} \oplus f_2^{(m,n)}\right).$$

For the functionality property of f (m, n) to be conserved, and are to be compatible: for any tuple α, if $f_1^{(m,n)}$ and $f_2^{(m,n)}$ are defined, they are to be equivalent. The orthogonal functions with nonoverlapping graphs are compatible.

Therefore, f (m, n)(α) equals one of the values $f_1^{(m,n)}(\alpha)$ or $f_2^{(m,n)}(\alpha)$, which is defined, or, in particular, is calculated first. All operations of composition are associative; the operation ⊕is also commutative. The following order of precedence of the operations of composition •, ∗, →, ⊕allows us to omit a number of parentheses when writing the functions.

5. The general form of function definition in FPTL is systems of functional equations of the form (1)

Xi = τi, i = 1, 2, …, n,

where Xi is the defined function, and τi is the term of the same arity and type as Xi given on the sets of the functional variables {X1, X2, …, Xn} and the basis functions {f1, f2, …}.

We construct the set of the terms inductively:

1) A functional variable or a basis function is the term of the same arity and type as the functional variable or the basis function.
2) If τ1 and τ2 are the terms, then (τ1Δτ2) are the terms, where $\Delta \in \{\bullet, *, \to, \oplus\}$. As indicated above, the arities of the terms τ1 and τ2 are to be in agreement for the applied operation of composition.
3) There are no other terms.

For strict basis functions, i.e., those whose value is not defined if at least one of the arguments is not defined, the operations of composition are monotone with respect to the graphs of the functions to which they are applied. Moreover, they are continuous [4, 9], which allows us to express the minimum solution of the system of functional equations (1) explicitly $X_i^{(\omega)} = \bigcup_{k=0}^{\infty} X_i^{(k)}$, i = 1, 2, …, n, where $X_i^{(0)} = \varnothing$ is the function defined nowhere with an empty graph and $X_i^{(k)} = \left[X_1^{(k)} \middle/ X_l \,\middle|\, l = 1, 2, \ldots, n\right]\tau_i$, here [A/X]B is the result of simultaneous substitution of A for all occurrences of X in B.

Two remarks need to be made concerning the form of a function definition in FPTL and its expressiveness. As mentioned before, aside from the universality requirement, the indicated operations of the composition of functions were mainly chosen based on the conventional mathematical way of defining a function in the form of recursive equalities whose right hand side could include the operation of the case analysis and substitution (substitution of functions for variables of the known function).

We consider an example of the recursive function definition

$$F(x,y) = \begin{cases} \text{if } P_1(x,y), \text{then } f_1(F(x,y), f_2(y)), \\ \text{if } P_2(x,y), \text{then } f_3(x,y), \\ \text{if } P_3(x,y), \text{then } F(f_4(x,y),y) \end{cases}$$

The functional scheme of F(x, y) has the following representation form (the function arity signs are omitted):

$$F = \left(P_1 \to \left(F * \pi_2^2 \bullet f_2\right) \bullet f_1\right) \oplus \left(P_2 \to f_3\right) \oplus \left(P_3 \to \left(f_4 * \pi_2^2\right) \bullet F\right)$$

Here, π_i^m (m≥0, 0≤i≤m) are the functions of argument choice (the basis functions): π_i^m (x1x2…xm) = xi and π_0^m (x1x2…xm) = λ(the empty tuple). Other basis functions are the constructors and the functions reciprocal to them (the destructors), which are induced when describing the data types.

The so-called parallel functions can be naturally presented in the language. The example of such functions is the voting function f(x1, x2, x3) known in telephony. Its value is defined if at least one pair of its arguments is known and their values are equivalent; in this case, the function value is the value of one of the arguments in this pair; otherwise, it is not defined. The functional scheme for this function has the form

$$f = \left(\pi_1^3 * \pi_2^3\right) \bullet P_{=} \rightarrow \pi_1^3 \oplus \left(\pi_2^3 * \pi_3^3\right) \bullet P_{=} \rightarrow \pi_2^3 \oplus \left(\pi_1^3 * \pi_3^3\right) \bullet P_{=} \rightarrow \pi_1^3$$

where P= is the propositional equality function.
This function can be directly expressed by the facilities of none of the sequential languages; to do this, it is necessary to organize a quasi-parallel computation of all its arguments; for instance, by checking, according to the counter or timer, if the obtained values are equivalent. The FPTL parallel operational semantics allows us to find the values of such functions correctly.

2.2 Data Definition
Any abstract data type can be represented in FPTL. Moreover, when constructing the type, the functions-constructors used and the functions-destructors reciprocal to them form the complete set of the basis functions together with the functions of argument choice, which means that any computable function over the datum of this type can be expressed by the FPTL facilities [2, 8]. In FPTL, data types, like functions, are defined by a system of relational equations using the operation of composition of functions and constructors introduced above. We give a simple example of defining the positive integers in FPTL.

```
Data NAT {
      Constructors {
            => Nat : O;
            Nat => Nat : succ;
      }
          NAT = O ⊕ NAT•succ;
}
```

The constructors introduced here and the destructors, which correspond to them implicitly and uniquely, form the complete set of the basis functions. Using them, any recursive function can be expressed over the NAT data set. In the given example, the construction NAT•succ is interpreted as the set {succ(x) | x∈NAT}. The destructors are implicitly introduced in the language together with the constructors. The destructors O-1 and succ-1 are interpreted as $O^{-1}(O) = \lambda$, $O^{-1}(succ) = \omega$; $succ^{-1}(succ(x)) = x$, $succ^{-1}(O) = \omega$.
Note the important practical characteristics of FPTL: the schematic form of function definition; the strict typing; the possibility to define parameterized functions and data; the language polymorphism which lies in the possibility to use functions and data in programs that are defined in other programming languages (C, Pascal, etc.).

FPTL has two semantics: the denotational semantics described above and the parallel operational semantics considered in the next section.

2.3 Model of Parallel Computation of Function Values
A parallel function evaluation model M defines a computation process as that of tree transformations [4]. At each step, the computation state is represented by a binary marked tree that satisfies the following requirements: (i) the leaves of the tree are marked by symbols of elements D∪{ω}, where D is a data universum and ωis a computable undefined value, and (ii) the inner nodes of the tree are marked either by the operation symbols •, ∗, →, ⊕or by functional terms. Without loss of generality, we assume that the function of interest X1 is determined by a system of functional equations

$$Xi = \tau i,\ i = 1, 2, \ldots, n, \quad (2)$$

where τi is a functional term containing only the variables X1, X2, …, Xn and the basic functions f1, f2, ….

The computation of the function value $X_1^{(min)}$, which is the first coordinate of the least solution of equation (2) in X1, for the argument given by a tuple d is represented as a sequence of states, with the initial state being a tree with two nodes. The root node of the tree is marked by the functional variable symbol X1, and the leaf node, by the argument d. The sequence of states has only one terminal state if the computation process successfully terminates. If this state is a one-node tree marked by some data d′∈D, the function value is said to be successfully evaluated with the result d'. If the terminal state is ω, the computation is said to terminate unsuccessfully. The endless computation process is considered unsuccessful. When evaluating a function, transitions from one state to another are determined by rules of tree transformations, which can be classified into two groups: rules for tree folding and rules for tree unfolding.

Tree transformation rules are specified as schemes of state variations and denoted as u′⇒u″, where u′ and u″ are state schemes. A state scheme differs from a particular state in that the nodes of the state tree in the scheme may be marked by the following metavariables: an arbitrary functional term t (possibly, with indices), an arbitrary state tree u, and arbitrary element d of D (possibly, with indices), a basic function f, and a functional variable Xi.

The result of the application of the rule u′⇒u″ to the state u is a tree obtained by replacing the subtree u' of the tree u by the tree u".

Fig 1 and Fig 2 show tree unfolding rules and tree folding rules, respectively. The correctness of rules 6–9 follows from the fact that the operation ⊕is applied only to orthogonal or compatible functions.

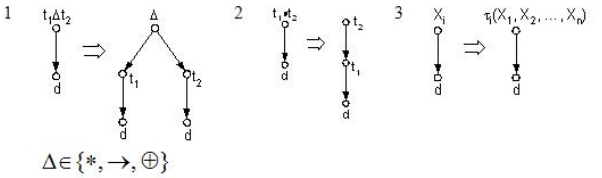


Fig.1. Tree unfolding rules

This model is not deterministic, since, generally, several rules can be applied to a state tree; hence, different computation sequences can be obtained depending on the rule applied. Note that this is a parallel model, since several rules can simultaneously be applied to isolated parts of the tree. The parallelism relies on the properties of the operations ∗, →, ⊕. In practice, this means that the computation processes develop independently along different branches of the computation state tree, which explains why this computation model was called asynchronous [4].

It is important to note that not any order of the application of the transformation rules results in the correct evaluation of function values. Such a case takes place, for example, in the evaluation of (t1⊕t2)(d) when we first attempt to evaluate t1(d) that is not defined and the computation process is endless, whereas the value t2(d) is defined. Thus, the correctness condition for the model implementation is the parallel (or

quasiparallel) evaluation of functions joined by the operation ⊕

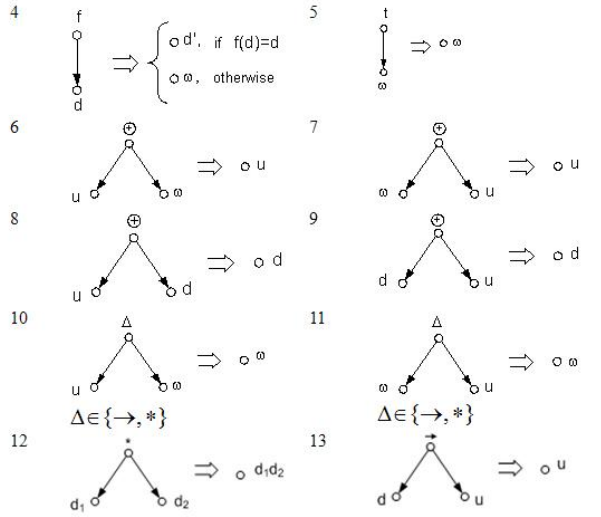


Fig. 2. Tree folding rules

It is important also to be able to stop needless computations. As can be seen from rules 6–11, if we get a value d different from ωor the value ωon one of the branches, the computation process along the other branch has to be stopped.

In addition, the model makes it possible to improve the computation efficiency by using look-ahead computations. If the amount of resources is sufficient, in the evaluation of (t1→t2)(d), we can evaluate the value t1(d) simultaneously with t2(d) trying to maximally parallelize the computation process.

These features of the computation model are fundamentally important when implementing the model on computer systems and when developing efficient scheduling algorithms for parallel execution of functional programs.

In nowadays realization of FPTL on multicore clusters this model was significantly improved in order to achieve effective realization [3].

3. TOOLS FOR PROGRAM DEVELOPMENT

An effective use of any programming language is impossible if its implementation does not contain tools designed for improving efficiency of the programming in this language. Many of these tools – support of the top-down and bottom-up development processes, syntax and type checking, debugging and testing tools, documentation means, and others – are universal. Modern programming environments for supporting programming processes, such as Visual Studio, Delphi, Rational Rose, etc., deal with a general technology of the programming, whereas some important aspects of the program development, such as meeting temporal (which is especially important in the development of parallel programs) and resource restrictions, program verification (i.e., proving that the program satisfies given specifications), and others, greatly depend on specific features of the programming language used and, therefore, constitute, as a rule, a specialized part of its programming environment. These specific program tools for supporting development of functional programs in the FPTL will be discussed below.

The process of problem solving consists of the following several stages [1]: (1) problem statement, (2) selection of the solution method or development of a new method, (3) development of an algorithm and programming, (4) selection of the architecture of a computing system, and (5) program execution. The creative character of the stages of the problem statement, search for solution, method and algorithm, program construction, etc., leaves little room to those aspects of the process of problem solving that have rational character and, hence, can be automated by means of a computer [1]. However, this does not exclude the use of special tools aimed at simplification and speed-up of these stages. The programming environment being developed is just a tool of this kind. It contains the following main elements:

- project organization block,
- bottom-up development support block,
- top-down development support block,
- verification block,
- program editor,
- syntax and type-checking block,
- structural analysis block,
- computational complexity estimation block,
- block of task-oriented equivalent transformations.

Under the project, we mean everything that is related to solving a given problem, starting from its statement and ending with the program designed for solving this problem. The project organization block ensures storing and management of all information related to the project, including various specifications, documentation, project development history (selection of main components – solution method and its implementation – of the problem solution process), and the like. The bottom-up development support block allows us to use in the development of a program some known solutions. This block includes two parts: one ensures interaction with libraries of subroutines written in other languages, and the other allows us to accumulate functional programs. The second part includes a database of functional programs, which contains programs themselves, their descriptions, and, possibly, various characteristics. In the future, this may be a knowledge database on problems. The top-down development support block is designed for the functional decomposition of the original problem into simpler subproblems, when the problem gradually reduces to language primitives. The problem solution is formed based on notions that can be interpreted and implemented in many ways, which are possibly not completely understood and will further be refined in terms of other notions until all intermediate notions introduced are implemented in terms of basic language concepts. It should be noted that the language itself has means for supporting the top-down development: it is possible to decompose the original problem (function) into simpler ones by introducing new functional variables and combining them by means of the composition operations.

The verification block is designed for searching for errors in the program specification and proving program correctness [10]. This problem includes the following subproblems:

- search for contradictions in specifications,
- proof of the totality and functionality of program functions,
- search for errors in the verification object,
- proof of the correspondence of the verification object to its specifications.

The verification method is based on the possibility of translating functional programs to the language of logic of the

first-order predicates. The program editor is a standard part of the program development environment, which ensures input and editing of the program text at the level of semantic language constructs. The syntax and type-checking block is responsible for the syntax correctness of the inputted language constructs and for the correctness of the program typification. The structural analysis block [3] allows us to estimate complexity of the functional program in terms of the recursiveness, cyclicity, mutual recursiveness, and nesting and to classify program constructs, which will further be used when scheduling parallel computations. This block makes it possible also to use graphic representations of functional programs. The computational complexity estimation block allows one to obtain numerical characteristics for the complexity of execution of a functional program by means of given complexity estimates of the basic functions used in the program [3]. The block of task-oriented equivalent transformations implements equivalent transformations of programs based on the calculus of functional program equivalence suggested in [3]. The aim of such transformations is to improve some program characteristics. The set of such transformations includes transformation to a form with the minimal time of the parallel execution, transformation to a form that avoids repeated function evaluations, and transformation to a form not containing look-ahead computations.

4. CONCLUSIONS

Just now FPTL has been extended in order to programmer can efficiently develop functional parallel programs related to linear algebra problems in which vector matrix and other operations are typical. It is well known that programming of this kind problems by using functional notation is no trivial task and special constructs are necessary for it in FPTL.

At the same time experimentation with various functional parallel programs is initiated on the multicore cluster which comprises 16 nodes with 4 processors each (two processors with two cores each) and with 10 Gbit/sec Infiniband communication channels.

Operating tools for efficient running functional programs on cluster has been developed strongly with methods and algorithms created for this purpose in [3].

REFERENCES

[1] V.P. Kutepov., “On Intelligent Computers and Large New-Generation Computer Systems”. *Journal of Computer and Systems Sciences International* vol. 35, no. 5, 1996.

[2] S.E. Bazhanov, V.P. Kutepov and D.A. Shestakov, “Functional Parallel Typified Language and Its Implementation on Clusters”, *Programming and Computer Software 31* (5)(2005).

[3] S. E. Bazhanov, V. P. Kutepov, D. A. Shestakov, and M. M. Vorontsov, “Structural Analysis and Planning of Processes of Parallel Execution of Functional Programs”, *Journal of Computer and Systems Sciences International*, vol. 44, no. 6, 2005.

[4] V.P. Kutepov and V.N. Fal’k, “Models of Asynchronous Evaluation of Functions in a Language of Functional Schemes”, *Programmirovanie*, 1978, no. 3.

[5] V.P. Kutepov and V.N. Fal’k, “Functional Systems: Theoretical and Practical Aspects”, *Kibern*., 1979, no. 1.

[6] V. P. Kutepov, “Flowgraph Calculus and Parallel Algorithms,” *Programmirovanie*, No. 6 (1976).

[7] V. P. Kutepov, “Extended Abstract of Doctoral Dissertation in Technical Science” (Mos. Pov. Inst., Moscow, 1982).

[8] V. P. Kutepov and V. N. Fal’k, “Directed Relations: Theory and Applications,” Izv. Ross. Akad. Nauk, Tekh. Kibern., No. 4, 5 (1994).

[9] V. P. Kutepov, *Arrangement of Parallel Computations on Systems* (MPEI, Moscow, 1988) [in Russian].

[10] V.P. Kutepov and I.I. Ul’yanovskii, *Verification of the Functional Program Development Process.*

An Efficient Recovery Scheme for Supercomputing Clusters and Grids*

Zizhong Chen[1, 2], Ming Yang[1], Monica Trifas[1], and Jack Dongarra[2]
[1]MCIS Department, Jacksonville State University
Jacksonville, AL 36265, USA
[2]Computer Science Department, University of Tennessee
Knoxville, TN 37996, USA
Email: zchen@cs.utk.edu

ABSTRACT

Checkpointing is a typical approach to tolerate failures in supercompuitng clusters and computational grids. Checkpoint data can be saved either in central stable storage, or in processor memory (as in diskless checkpointing), or local disk (replacing memory with local disk in diskless checkpointing). But where to save the checkpoint data has a great impact on the performance of a checkpointing scheme. Fault tolerance schemes with higher efficiency usually choose to save the checkpoint data closer to the processor. However, when failures are handled from application level, the storage hierarch of a platform is often not available at the fault tolerance scheme design time. Therefore, it is often difficult to decide which checkpointing schemes to choose at the fault tolerant application design time. In this paper, we demonstrate that, good fault tolerance efficiency can be achieved by adaptively choosing where to store the checkpoint data at run time according to the specific characteristics of the platform. We analyze the performance of different checkpoint schemes and propose an efficient adaptive scheme to incorporate fault tolerance into parallel applications.

Keywords: Checkpoint, Fault Tolerance, Parallel and distributed Computing, Cluster Computing, Grid Computing

1. INTRODUCTION

Checkpointing is a typical approach to tolerate failures in supercomputing clusters and computational grids [8]. Checkpoints can often be taken either from the system level or from the application level. However, when checkpoints are taken from application level, most fault tolerance schemes proposed in literature are *non-adaptive* in the sense that the fault tolerance schemes incorporated in applications are either designed without incorporating system environments (such as the amount of available memory and the local and network I/O bandwidth, etc) or designed only for a specific system environment. From the application point of view, fault tolerant high performance applications need to be able to achieve high performance under different system environments with as low performance overhead as possible. In order to achieve high reliability and survivability with low performance overhead, the fault tolerance schemes in such applications need to be adaptable to different (or dynamic) system environments.

In this paper, we demonstrate that, good fault tolerance efficiency can be achieved by adaptively choosing where to store the checkpoint data at run time according to the specific characteristics of the platform. We analyze the performance of different checkpoint schemes and propose an efficient adaptive scheme to incorporate fault tolerance into parallel applications.

* This research was supported in part by the Los Alamos National Laboratory under Contract No. 03891-001-99 49.

Applying this scheme to self-adaptive numerical software such as LAPACK for Clusters [2] will result in self-adaptive fault tolerant numerical libraries. Applications that call this type of self-adaptive fault tolerant numerical libraries will be able to survive certain processor failures transparently with very low performance overhead.

The rest of this paper is organized as follows. Section 2 defines the problem we are targeting. Section 3 analyzes the performance of several static checkpointing schemes. Section 4 presents a self adapting application level fault tolerance scheme for high performance grid computing. In Section 5, experimental and simulation results are presented. Section 6 concludes the paper.

2. APPLICATION LEVEL FAULT TOLERANCE

To define the problem we are targeting and clarify the differences with the system level fault tolerance approaches, in this section we first specify the type of failures we are focusing on and then briefly introduce FT-MPI, a fault tolerant version Message Passing Interface that supports application level fault tolerance.

Assume the target computing systems have many nodes which are connected by network connections. Each node has its own memory and local disk. There is at least one processor on each node and only one application process on each processor. Assume the target application is optimized to run on a fixed number of processes. Unlike in traditional algorithm-based fault tolerance which assumes a failed process continues to work but produce incorrect results, in this work we assume a *fail-stop* failure model. In a fail-stop failure model, the failed process is assumed to stop working and all data associated with the failed process are assumed to be lost. The surviving processes can neither send nor receive any message from the failed processes.

Current parallel programming paradigms for high-performance distributed computing systems are typically based on the Message-Passing Interface (MPI) specification [9]. However, the current MPI specification does not specify the behavior of an MPI implementation when one or more process failures occur during runtime. MPI gives the user the choice between two possibilities of how to handle failures. The first one, which is the default mode of MPI, is to immediately abort all the processes of the application. The second possibility is just slightly more flexible, handing control back to the user application without guaranteeing that any further communication can occur.

FT-MPI [6] is a fault tolerant version of MPI that is able to provide basic system services to support fault survivable applications. FT-MPI implements the complete MPI-1.2 specification, some parts of the MPI-2 document and extends

some of the semantics of MPI for allowing the application the possibility to survive process failures. FT-MPI can survive the failure of *n-1* processes in an *n*-process job, and, if required, can re-spawn the failed processes. However, the application is still responsible for recovering the data structures and the data of the failed processes.

3. STATIC CHECKPOINTING

When building fault tolerant applications with FT-MPI, many fault tolerance schemes can be used. In this section, we analyze both the performance and the storage requirement of different checkpointing schemes that can be used with FT-MPI. To simplify the analysis, we only discuss the case to tolerate single processor failure.

Assume the checkpointing is performed in a parallel system with p processors and the size of checkpoint on each processor is m bytes. It takes $\alpha+\beta x$ to transfer a message of size x bytes between two processors regardless of which two processors are involved and. α is often called latency of the network. $1/\alpha$ is called the bandwidth of the network. Assume the rate to calculate the XOR of two arrays is γ seconds per byte. We also assume that it takes $\alpha+\beta x$ to write x bytes of data into the stable storage. The I/O band width to local disk is assumed to be $1/\zeta$. Our default network model is the duplex model where a processor is able to concurrently send a message to one partner and receive a message from a possibly different partner. The more restrictive simplex model permits only one communication direction per processor. We also assume that disjoint pairs of processors can communicate each other without interference each other.

3.1 CSSC: Central Stable Storage Checkpoint

Today's long running scientific applications typically tolerate failures by checkpoint/restart approaches in which all process states of an application are periodically saved into stable storage. The advantage of this approach is that it is able to tolerate the failure of the whole system. However, in this approach, if one process fails, usually all surviving processes are aborted and the whole application is restarted from the last checkpoint. The major source of overhead in all stable-storage-based checkpoint systems is the time it takes to write checkpoints to stable storage [12]. The checkpoint of an application on a, say, ten-thousand-processor computer implies that all critical data for the application on all ten thousand processors have to be written into stable storage periodically, which may introduce an unacceptable amount of overhead into the checkpointing system. As the number of processors in the system increases, the total number of process states that need to be written into the stable storage also increases linearly. Therefore, the fault tolerance overhead increases linearly.

When the size of checkpoint on each processor is m bytes, the total size of checkpoint for all processors is pm bytes. Therefore, the amount of stable storage needed for the central stable storage checkpoint scheme is pm bytes. Without the support of a parallel file systems, to write all checkpoint data on all processors into the central stable storage, the time T_{cssc} it takes can be estimated by

$$T_{cssc} = \alpha + p * \beta m \approx p\beta m$$

when m is relatively large.

When there is a parallel file system in the system, p in the above formula represents the number of processors each file server serves.

3.2 MBPC: Memory-Based Parity Checkpoint

Diskless checkpointing [12] is a technique to save the state of a long running computation on a distributed system without relying on stable storage. Memory-based parity checkpoint is one form of the diskless checkpointing. With memory-based parity checkpoint, each processor involved in the computation stores a copy of its state locally, either in memory. Additionally, encodings of these checkpoints are stored in local memory of some processors. When a failure occurs, each live processor may roll its state back to its last local checkpoint, and the failed processor's state may be calculated from the local checkpoints of the surviving processors and the checkpoint encodings. By eliminating stable storage from checkpointing and replacing it with memory and processor redundancy, memory-based parity checkpoint removes the main source of overhead in checkpointing on distributed systems [12].

By breaking up a large message of size m into s smaller segments and sending these smaller messages through the network by a pipelining style, the time to perform diskless checkpoint can be modeled by

$$T_{mbpc} = (p-1+m/s)(\alpha+\beta s+\gamma s)$$

When

$$s = \sqrt{\frac{m\alpha}{(p-1)(\beta+\gamma)}}$$

T_{mbpc} achieves its minimum:

$$T_{mbpc} = (p-1)\alpha + (\beta+\gamma) + 2\sqrt{(p-1)\alpha(\beta+\gamma)m}$$
$$= (\beta+\gamma)m * \left(1 + 2\sqrt{\frac{(p-1)\alpha}{(\beta+\gamma)m}} + \frac{(p-1)\alpha}{(\beta+\gamma)m}\right)$$
$$\approx (\beta+\gamma)m$$

when m is relatively large and p is relatively small.

If the size of checkpoint for each processor is m bytes, the memory overhead for the memory-based parity checkpoint scheme is m bytes.

3.3 DBPC: Disk-Based Parity Checkpoint

Many applications, such as HPL benchmark [4], achieve higher efficiency when most of the processor memory is used for the application. Reserving memory for checkpointing purpose often degrades the performance. However, if there is a local disk associated with the processor, free local disk storage can be used to store the checkpoint data. The checkpointing algorithm works the same way as the memory-based parity checkpoint except that the local disk is used to replace the memory.

By using the same pipelined XOR calculating algorithm as in memory-based parity checkpoint scheme, the time to perform checkpointing can be approximated by

$$T_{dbpc} \approx (\beta+\gamma+\zeta)m$$

when m is relatively large and p is relatively small.

In the disk-based parity checkpoint scheme, if the size of checkpoint for each processor is m bytes, the local disk storage overhead for the disk-based parity checkpoint scheme is m bytes.

3.4 MBCM: Memory-Based Checkpoint Mirroring

When processor memory is used to store the checkpoint data, another possibility is to organize all computation processors as pairs (assume there are even number of computation processors). The two processors in a pair are neighbors of each

other. Each processor first takes a local in-memory checkpoint and, at the same time, sends a copy of its local checkpoint to its neighbor processor.

Under the duplex network model where a processor is able to concurrently send a message to one partner and receive a message from a possibly different partner, the time to perform checkpoint mirroring can be approximated by

$$T_{mbcm} = \alpha + \beta m \approx \beta m$$

when m is relatively large.

If the size of checkpoint for each processor is m bytes, the memory overhead for the memory-based checkpoint mirroring scheme is $2m$ bytes.

3.5 DBCM: Disk-Based Checkpoint Mirroring

When there is a local disk associated with each processor, the local disk can be used to replace the memory used in the memory-based checkpoint mirroring scheme. This scheme can be called as disk-based checkpoint mirroring scheme.

Under the duplex network model, the time to perform disk-based checkpoint mirroring can be approximated by

$$T_{dbcm} = \alpha + \beta m + \zeta m \approx (\beta + \zeta) m$$

when m is relatively large.

In the disk-based checkpoint mirroring scheme, if the size of checkpoint for each processor is m bytes then the local disk storage overhead for the disk-based checkpoint mirroring scheme is $2m$ bytes.

4. SELF-ADAPTIVE CHECKPOINTING

From Section 3, we have seen that each fault tolerance scheme has its own advantages and disadvantages. However, different systems have different resource characteristics. What is the best way to incorporate different fault tolerance schemes into applications so that the reliability and survivability is as high as possible while the performance overhead is as low as possible?

From the application point of view, it is desirable that fault tolerant high performance applications is able to achieve both high performance and high reliability (survivability) with low fault tolerance overhead no mater under which kind of system environments it is running. To achieve this goal, the best strategy would be to adaptively choose the fault tolerance schemes in applications based on different (or dynamic) system environments that the applications are running.

The key idea of our recovery framework is the adaptivity of our checkpoint scheme to different system environments. Our adaptive scheme is similar to Vaidya's two-level recovery scheme [14] in that both schemes combine the central stable storage checkpoint scheme with other higher efficiency checkpoint schemes such as diskless checkpointing. However Vaidya's recovery technique is static. He consider the availability of the memory and the local disk storage at the software design time, but after the design is finished, the software will never need to check the information of the hardware architecture (such as number of available processors, amount of memory and local disk storage) again. Thus we classify his scheme as static scheme. However, in our scheme, the software will have to check the information of the hardware architecture (such as number of available processors, amount of memory and local disk storage) to decide the optimal checkpoint scheme. Thus, we regard our scheme as adaptive rather than static.

The application of this self-adaptive fault tolerance framework to self-adaptive numerical software such as LFC [2] will result in self-adaptive fault tolerant numerical libraries. Applications that use this kind of self-adaptive fault tolerant numerical libraries is able to survival certain processor failures transparently with very low performance overhead.

4.1 A Simple Self Adaptive Recovery Scheme

What checkpoint scheme is the best for a specific system is often affected by many factor such as the amount of available storage of each type, the overhead of each checkpoint scheme, the failure rate and distribution of the system, the characteristics of the application, and the number of available processors for this application, etc. At the present stage, we only consider

- The size of checkpoint;
- The amount of available memory;
- The amount of available local disk storage;
- The amount of central stable storage;

If one type of storage is not available in the system, then we assume there are zero bytes of that type of storage in the system. We also assume that a node failure also means that both its memory and its local disk become unavailable.

The five candidate basic checkpoint schemes that we consider at the present time are

- **CSSC:** central stable storage checkpoint scheme
- **DBPC:** disk-based parity checkpoint scheme
- **DBCM:** disk-based checkpoint mirroring scheme
- **MBPC:** memory-based parity checkpoint scheme
- **MBCM:** memory-based checkpoint mirroring

In the self-adaptive checkpointing scheme we first check the amount available free memory, free local diskless storage, and free central stable storage. We then use this information to choose the best basic recovery scheme. At the present time, we decide the checkpoint frequency manually. If we can somehow check the MTBF (or the failure rate) of the system in the future, we will use it to decide the checkpoint frequency.

It has been shown both from our experiments and in literature [3, 10, 11, 12, 13, 14] that the memory-based checkpoint mirroring scheme usually performs better than memory-based parity checkpoint scheme which usually performs better than disk-based checkpoint mirroring scheme. Disk-based checkpoint mirroring scheme usually performs better than disk-based parity checkpoint scheme which performs better than central stable storage checkpoint scheme. Based on this fact, we propose to use the algorithm in Figure 1 to decide which simple checkpoint scheme to choose. By making decisions at run time, we get the opportunity to know more information about the platform the application will execute than making decisions at the application design time. Therefore, we get the opportunity to make better decisions. This is why we can get better performance in a self adapting fault tolerance scheme.

```
if ( there is enough memory for MBCM) {
      use MBCM;
} else if ( there is enough memory for MBPC ) {
      use MBPC;
} else if ( there is enough disk for DBCM ) {
      use DBCM;
} else if ( there is enough disk for DBPC ) {
      use DBPC;
} else if ( there is enough central stable storage )   {
      use CSSC;
} else {
      there is no enough storage to store checkpoint;
}
```

Fig.1. A simple self adaptive fault tolerance scheme

4.2 Performance Analysis

In this section, we analyze the overhead of the proposed self adapting application level fault tolerance scheme.

The fault tolerance overhead for the self adapting fault tolerance scheme includes two part: the overhead for gathering system information and making a decision on which simple scheme to use and the overhead for actually performing the checkpoint. Assume the time to gather system information and make a decision is $T_{decision}(p)$ and the time to perform the checkpoint is $T_{adaptive-checkpoint}(p,m)$.

The self-adapting checkpoint scheme makes a decision on which simple checkpoint scheme to choose according the size of the checkpoint and the amount of each type of storage available. Consider a simplified case where each processor has the same amount freely available memory, and local disk storage. Let S_m denote the amount of the local free memory for a processor, S_d denote the amount of the local free disk storage of a processor, and S_c denote the amount of central stable storage. Assume $S_m \le S_d \le S_c / p$, then

$$T_{adaptive-checkpoint}(p,m) = \begin{cases} T_{decision}(p) + \beta m, & \text{if } m \le S_m/2 \\ T_{decision}(p) + (\beta+\gamma)m, & \text{if } S_m/2 < m \le S_m \\ T_{decision}(p) + (\beta+\zeta)m, & \text{if } S_m < m \le S_d/2 \\ T_{decision}(p) + (\beta+\gamma+\zeta)m, & \text{if } S_d/2 < m \le S_d \\ T_{decision}(p) + p\beta m, & \text{if } S_d < m \le S_c/p \end{cases}$$

$T_{decision}(p)$ is the time for gathering system information and making a decision, which is often negligible compared with the overhead to perform the actually checkpoint. Compared to basic non-adaptive schemes such as the central stable storage checkpoint scheme in which the time for one checkpoint is $p\beta m$, the adaptive scheme usually has better performance unless $S_c / p < m$. When $S_c / p < m$, there is no enough storage to store any checkpoint.

Schemes with low fault tolerance overhead tend to use local (or neighbor) memory or local (or neighbor) disk instead of central stable storage to store checkpoint data. However, it is usually unclear about what is the amount of local storage that can be used to store the checkpoint data until the program execution time. By postponing the time to make decisions to the program execution time, we get the opportunity to use as much local and neighbor storage as possible to store the checkpoint data. Therefore, we are able to get better performance by adapting the fault tolerance scheme to system environments at run time.

5. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed self adapting fault tolerance scheme.

5.1 Experimental Results

In this subsection, we compare the time for one checkpoint of the following two checkpoint schemes

- **MBPC:** The neighbor memory-based parity checkpoint scheme
- **SSAC:** The simple self adapting checkpointing scheme which chooses the best scheme from the five basic schemes at run time according to the amount of different storage available.

The application we used to perform experiment is the PCG code described in [1]. The number of simultaneous processor failures we want to survive is one. The total number of processors we used in PCG is sixteen. The programming environment we used is FT-MPI [5, 6, 7]. All experiments were performed on a cluster of 32 Pentium IV Xeon 2.4 GHz dual-processor nodes. Each node of the cluster has 2 GB of memory and runs the Linux operating system. The nodes are connected with a Gigabit Ethernet. The timer we used in all measurements is *MPI_Wtime*.

Table 1. Performance of the simple self-adaptive checkpointing scheme for PCG

size of checkpoint	T_SSAC (Seconds)	T_MBPC (Seconds)
100	2.21	2.55
200	4.55	5.09
300	6.56	7.66
400	8.91	10.10
500	10.58	12.61
600	15.30	15.20
700	17.85	17.75
800	20.40	20.11

Table 1 reports the time for performing one checkpoint for both the SSAC and the MBPC schemes. By changing the input problem size in PCG, we varied the amount of data that need to be checkpointed from 100 MBytes to 800 MBytes. The results in Table 1 indicate that the SSAC scheme performs better than the MBPC scheme when the size of checkpoint is less than 500 MBytes. However, when the size of checkpoint is larger than 500 MBytes, the SSAC scheme performs approximately the same as the MBPC scheme. This is because, when the size of checkpoint is less than 500 MBytes, the SSAC scheme detects that a processor can store both a copy of its own checkpoint data and a copy of its neighbour processor's checkpoint data in its local memory. Therefore, the use the memory-based checkpoint mirroring scheme (which has lower performance overhead but high memory overhead than MBPC) is recommended. However, when the size of checkpoint is larger than 500 MBytes, the SSAC scheme detects that there is no enough local memory for a processor to store both its own checkpoint data and his neighbour processor's checkpoint data, therefore, choose to store only its own checkpoint data in his local memory and at the same time store the parity of all local checkpoint data into the memory of another dedicate processor, which is exactly what the MBPC scheme does.

5.2 Simulation Results

In this subsection, we simulate the performance of the

self-adaptive checkpointing scheme by choosing appropriate parameters for $T_{adaptive-checkpoint}(p,m)$ in Section 4.2.

Fig 2 shows a simulated result for the performance of the self-adapting fault tolerance scheme. In this simulation, $\beta=20*10^{-9}$, $\gamma=5*10^{-9}$, $\zeta=13*10^{-9}$, $p=5$, $T_{decision}(p)=0.1$ seconds, S_m=400 MBytes, and S_d=20 GBytes.

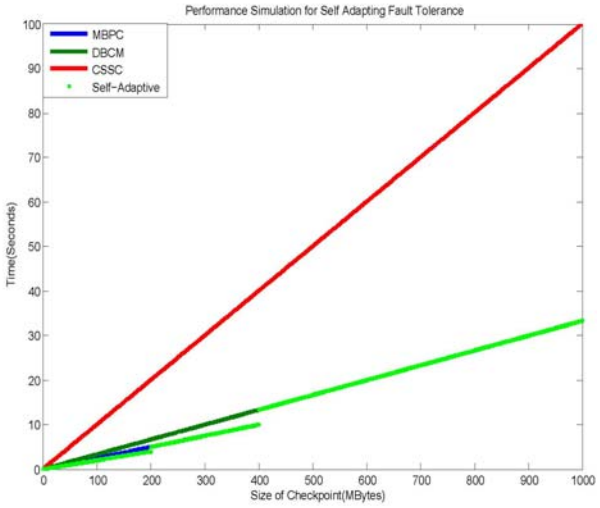


Fig. 2. Performance simulation for the self-adaptive chechpointing scheme

From Fig 2, we can see that the self-adapting fault tolerance scheme always choose the best available simple checkpoint schemes according to the size of the checkpoint and the amount of storage available. In particular, if the application designer is not sure whether there are enough memory or local disk storage to store the checkpoint at the application design time and conservatively choose the central stable storage checkpoint approach as the fault tolerance scheme, Fig 2 demonstrates that the fault tolerance overhead can be several times higher than the self-adapting fault tolerance scheme.

6. CONCLUSIONS

In this paper, we analyzed the performance of different checkpoint schemes and proposed an efficient adaptive scheme to incorporate fault tolerance into MPI applications. Experimental results demonstrated that good fault tolerance efficiency can be achieved by adaptively choosing where to store the checkpoint data at run time according to the specific characteristics of the platform.

REFERENCES

[1] Z. Chen, G. E. Fagg, E. Gabriel, J. Langou, T. Angskun, G. Bosilca, and J. Dongarra. "Fault tolerant high performance computing by a coding approach", *Proceedings of the ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*, PPOPP 2005, June 14-17, 2005, Chicago, IL, USA. ACM. 2005.

[2] Z. Chen, J. Dongarra, P. Luszczek, and K. Roche, "Self-adapting software for numerical linear algebra and LAPACK for clusters", *Parallel Computing*, (11-12), pp.1723–1743, November-December 2003.

[3] T. Chiueh and P. Deng. "Evaluation of checkpoint mechanisms for massively parallel machines", *FTCS*, pp .370–379, 1996.

[4] A. Petitet, R. C. Whaley, J. Dongarra, and A. Cleary. "HPL - A Portable Implementation of the High Performance Linpack Benchmark for Distributed Memory Computers". http://www.netlib.org/benchmark

[5] G. E. Fagg and J. Dongarra. "FT-MPI: Fault tolerant MPI, supporting dynamic applications in a dynamic world" In *PVM/MPI 2000*, pp.346–353, 2000.

[6] G. E. Fagg, E. Gabriel, G. Bosilca, T. Angskun, Z. Chen, J. Pjesivac-Grbovic, K. London, and J. J. Dongarra. "Extending the MPI specification for process fault tolerance on high performance computing systems", *Proceedings of the International Supercomputer Conference*, Heidelberg, Germany, 2004.

[7] G. E. Fagg, E. Gabriel, Z. Chen, , T. Angskun, G. Bosilca, J. Pjesivac-Grbovic, and J. Dongarra, "Process fault-tolerance: Semantics, design and applications for high performance computing",*International Journal of High Performance Computing Applications*, 2005.

[8] I. Foster and C. Kesselman,*The Grid: Blueprint for a New Computing Infrastructure*, Morgan Kauffman, San Francisco, 1999.

[9] "Message Passing Interface Forum", "MPI: A Message Passing Interface Standard", *Technical Report ut-cs-94-230*, University of Tennessee, Knoxville, Tennessee, USA, 1994.

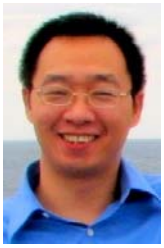
[10] J. S. Plank and K. Li. *Faster checkpointing with n+1 parity. FTCS*, pp.288–297, 1994.

[11] J. S. Plank. "Improving the Performance of Coordinated Checkpointers on Networks of Workstations using RAID Techniques", *The 15th Symposium on Reliable Distributed Systems*, pages 76–85, 1996.

[12] J. S. Plank, K. Li, and M. A. Puening, "Diskless checkpointing", *IEEE Trans. Parallel Distrib. Syst.*, 9(10), pp.972–986, 1998.

[13] L. M. Silva and J. G. Silva. *An experimental study about diskless checkpointing. EUROMICRO'98*, pp.395–402, 1998.

[14] N. H. Vaidya. "A case for two-level recovery schemes", *IEEE Trans. Computers*, 47(6),pp.656–666, 1998.



Zizhong Chen is an Assistant Professor of Computer Science at Jacksonville State University, AL, USA. He received his Ph.D. in Computer Science from the University of Tennessee, Knoxville, TN, USA, in 2006, under the direction of Jack J. Dongarra. His research interests include high performance computing, parallel and distributed processing, cluster and grid computing, and large scale scientific and engineering computing.

Object-oriented Environment for Parallel Programming of Multicore Clusters Based on Flowgraph Stream Parallel Programming Language*

V.P. Kutepov[1], D.V. Kotlyarov [2], V.N. Malanin [3], N.A. Pankov[4]
Department of Applied mathematics, Moscow Power Engineering Institute (Technical University)
ul. Krasnokazarmennaya 13, Moscow, 111250 Russia
Email: [1]KutepovVP@mpei.ru, [2]KotlyarovDV@mpei.ru, [3]MalaninVN@mpei.ru, [4]N.Pankov@appmat.ru

ABSTRACT

In this paper we examine implementation of an object-oriented environment for parallel programming for Multi-core clusters based on Flowgraph Stream Parallel Programming Language that combines simple but powerful way to represent parallelism of real world systems.

Keywords: FSPPL, Parallel Programming, Object-Oriented Programming

1. INTRODUCTION

Today object-oriented approach is very popular for the development of complex software. The basic principles of object-oriented software development (OOSD): inheritance, encapsulation and polymorphism made it possible to significantly decrease size of the code and increase its reusability. But one of the main factors that makes OOSD the leading approach to software development is the existence of some well-defined methods of object-oriented design that bring together software design and implementation phases and simplify software modification.

These methods focus on software architecture based on modules, derived from the types of the objects a system works with. But the traditional sequential operational semantics of object-oriented (OO) languages based on sequential procedure call is very restricted when user makes attempt of modeling complicated asynchronous and parallel processes in a behavior of real system.

Today the main way to implement parallelism in OO languages is to use special technique based on notion of process. But using this technique is a very difficult task, which requires complex modification of sequential object-oriented program by introducing special-purpose process oriented objects.

As for parallel programming for distributed environments (clusters, grid) the object-oriented approach had delivered some new technologies that significantly simplify building of complex software systems with remote calls between their elements (CORBA, .NET Remoting, etc). However being low-level these technologies are also very restrictive for efficient programming of parallel distributed systems.

Our project is aimed to develop the object-oriented environment for parallel programming that combines simple but powerful way to represent parallelism of real world systems based on Flowgraph Stream Parallel Programming Language (FSPPL) [1] and object-oriented approach to design programming systems.

* This project is supported by the Russian Foundation for Fundamental Research (No. 06-01-00817).

2. FSPPL

Our project is based on the concept of decompositional parallel programming developed in FSPPL[1,5].

According to this concept a parallel program represents a multitude of components connected by data that are program versions of subtasks, which were introduced within the decomposition of a complex task into subtasks. The data dependency relation between them is explicitly represented in flowgraph parallel program (PP) by introducing a graph-scheme (GS). The data dependencies between components of a PP are exposed as typified connections between inputs and outputs of the components.

Terms of scheme and subscheme are used to give user easy tools for building PP by “top-down”; decomposition process reflecting hierarchical structure of PP.

Most important features of FSPPL and its PP designing technology are:

1) FSPPL is module-like (component-like) parallel programming language that allows to reflect decomposition process of program development via its GS, as well as process of component “packing” (“top-down” design) from ready components.
2) FSPPL is a multi-language programming system, as for module subtasks programming in the same PP can be used various sequential languages (C++, Pascal and so on). Management of data flows between module subtasks doesn’t require any efforts from programmer.
3) FSPPL supports visual development of PP. Moreover, programmer can also use traditional textual program representation.

All these FSPPL features tremendously simplify process of complex PP development, analysis and debugging. FSPPL has more opportunities for parallelism representation than MPI, PVM, etc.

The following forms of parallelism that objectively present in different tasks [1] are easily represented in FSPPL:

- parallelism of data-independent fragments;
- multiple data parallelism (SIMD parallelism by Flinn) that is represented by application of PP (or its fragment) to a multitude of independent input data and that is implemented through multi-pipe parallel execution of PP,
-flow dependent parallelism, when the input data are considered as some kind of consequences.

FSPPL naturally combines the opportunities of gross-grain parallelism representation (that is realized at the level of the GS and introducing modules) and fine-grain parallelism that is represented in subprograms of modules and can be implemented by multithreading.

Our experience in FSPPL programming shows that FSPPL allows to build adequate and often straight structure models of mass-service networks, distributed and many component systems, we have a positive experience in describing on FSPPL the distributed control processes of flexible automated manufactures, airports, etc, as well as multi-component program systems, where information relations are structured and permanent[2].

FSPPL was implemented on a number of multicomputer and multiprocessor systems in particular clusters. The main goal of the current implementation is to integrate FSPPL into OO environment to enable developer to use all the benefits of OO technology and to deliver the high level object-oriented environment for parallel programming.

3. EMBEDDING FSPPL INTO OBJECT-ORIENTED ENVIRONMENT

Reusability of the code in object-oriented programming can be reached at different levels of abstraction starting from procedures, data structures, and classes and up to logically and physically connected sets of classes. Using these systems of classes in architecture of an application implies using of built-in object interacting schemas in runtime. These systems of classes delivering services in some area are usually called integrated libraries.

We've adopted the idea of integrated library to embed principles of FSPPL into object-oriented environment. Flowgraph Parallel Program (FGPP) implemented with the library is called object-oriented FGPP (OOFGPP).

To build the integrated library for flowgraph stream parallel programming we have applied methods of object-oriented analysis for abstract FGPP, its syntax and parallel semantics. Using object-oriented decomposition we constructed the set of base classes that describe main objects of FGPP: scheme, module, conjunctive input group (CIG), conjunctive output group (COG), input and output buffers[1,5] and defined mechanisms of their interaction as private methods.

Now to build the OOFGPP developer has to implement a number of abstract classes exposed by the library.
The embedding of FSPPL into OO environment enables developer to treat elements of PP as objects that allows using OO mechanisms such as polymorphism, encapsulation and inheritance while designing the PP. The largest impact this causes on the structure of data flows between modules: that is now the objects can be sent between modules as usual data. This implies that developer can send objects of different classes derived form one parent class from one module to another and depending on class different methods can be applied to this object inside module procedure due to polymorphism.

While designing the library we used the most general constructions that are available in any modern object-oriented platform. In current implementation we have chosen .NET CLR platform to build it.

For effective usage of this library it's important to deliver a full range of instruments that covers the whole process of OOFGPP design, implementation and execution on a target system. In the next part of the paper we will describe the developed environment for parallel programming based on the integrated library that includes all those instruments.

4. OBJECT-ORIENTED ENVIRONMENT FOR PARALLEL PROGRAMMING

The following requirements in implementation of the described above concept and language tools of object-oriented parallel programming were taken into account:

1) Architecture of the environment should be built on component basis with strict division of the functions between them. Specifically, the following functions are strictly distinct in the developed environment:
   a) support of parallel program development process,
   b) remote access organization,
   c) management of parallel program execution process on cluster,
   d) management of processes and threads on multi-core cluster.
2) The environment should use original algorithms for management of the processes and cluster load, which allow to support dynamically the effective usage of resources and decrease parallel program execution time [3].
3) The environment should be built as open and expandable, in particular the development of subsystem for fault tolerance ensuring parallel cluster work is carried out now as a new component of it.
4) The software should have portability in its software realization and make availability to be applied on different computer platforms with different OS.

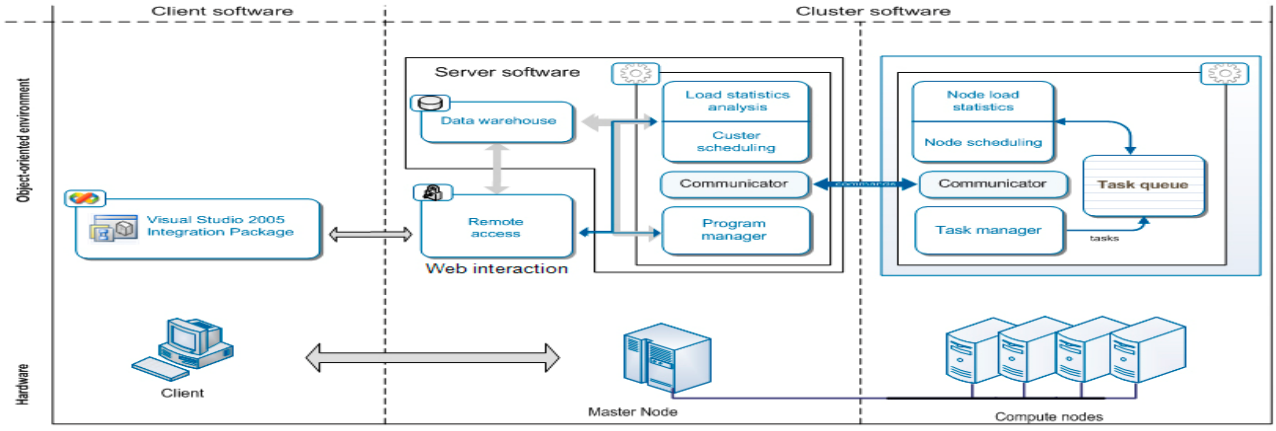


Fig.1. Object-oriented environment for parallel programming architecture

Let's briefly review the components of the developed environment.

5. ENVIRONMENT COMPONENTS

5.1 Client Software: FSPPL Integration Package

This component is intended for managing interaction between user and the system and it completed with three modules: module for development of OOFGPP, module of cluster configuration, module of control of PP execution.

The module for development of OOFGPP provides a parallel program project in Microsoft® Visual Studio® 2005 that fully complies with the developed principles of design and realization of the parallel distributed programs using the FSPPL. The module also contains the specialized editor of the graph structures for creating and editing of the parallel programs' schemes. Program code in conventional programming language (VB, MC++, C#, J#) is generated on the created schemes.

The module of cluster configuration provides services for setting the parameters of PP execution on cluster. It allows developer to design "initial scission" of the parallel program's scheme. The user operating with the data on the current cluster configuration creates special files that are attached to the project and may be used on the startup of execution (the analogue of machine file for MPI)[4].

The module of control of PP execution provides data on load of the remote cluster for user and allows him to control the execution process of the parallel program. The user interface of the package integrated into Microsoft Visual Studio 2005 is shown on Fig.2

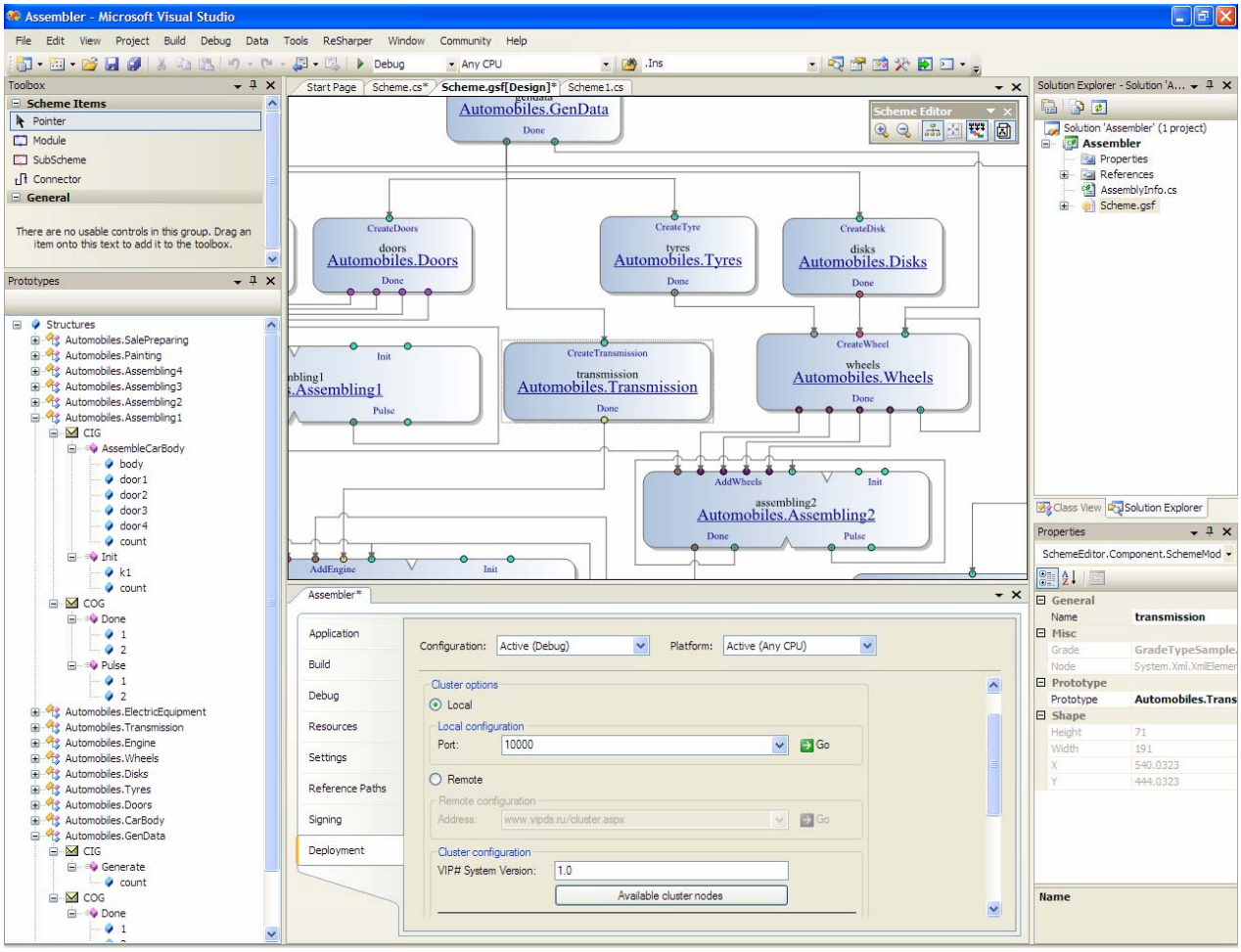


Fig.2. FSPPL Integration package

5.2 Web Interaction

This component is a layer between the client software and the cluster software. The component is a Web-service performing two functions:

- receiving user commands for the cluster software and initiating appropriate actions of the Execution Server component of the cluster software;
- providing to the client software an access to the data on cluster's load and task completion status.

The component has access to the system database, which contains data on registered users and their tasks which were performed on the target cluster.

5.3 Cluster Software: Execution Server

This component is needed for centralized cluster management. It includes the following modules:

- Program Manager, that uploads programs for execution, performs centralized management of the nodes, dispatches commands for launching, pausing, resuming and deleting parallel programs during execution process;
- cluster software administration tools, that enables remote administration of cluster nodes. The main functions are detecting available nodes, installing node software on remote nodes, starting and stopping node software on remote nodes, enabling/disabling scheduling on cluster
- Scheduler Server, that controls scheduling subsystem of cluster software. The module analyses the cluster load

statistics, data transfer and current configuration of the executing program, and makes decision on moving the tasks from one node to another in cases of getting prognostic information that the node will be overloaded and that the cluster scheduler should balance cluster load.

5.4 Node Software

Node software includes necessary functionality for the support of operational semantics of FSPPL. The component receives data from other cluster nodes and propagates the tasks for execution.

Scheduling of these tasks' execution is managed by the Node Scheduler and is based on the data on the node load statistics[4].

If overloading cannot be resolved on the node, local scheduler tries to move task(tasks) to another node by informing cluster scheduler.

6. CONCLUSIONS

At present time developed software has been experimentally tested on up to 16-node cluster with 64 cores. Now we work on further optimization of the software and development of additional subsystems such as fault-tolerance.
Developed software environment is included in the cycle of laboratory works for teaching students and staff of Moscow Power-Engineering Institute and other Moscow universities by program, supported by Intel Corporation, which is aimed to wide practical usage of multicore computers and cluster systems.

REFERENCES

[1] V.P. Kutepov, "On Intelligent Computers and Large New-Generation Computer Systems", *Journal of Computer and Systems Sciences International*, Vol. 35, No. 5, 1996.

[2] D.V. Kotlyarov, V.P. Kutepov, M.A. Osipov, "Flowgraph Stream Parallel Programming and Its Implementation on Cluster Systems", *Journal of Computer and Systems Sciences International*, 2005, Vol. 44, No. 1, pp. 70-89.

[3] V.P. Kutepov, "Scheduling Parallel Processes and Load Balancing in Large-Scale Computing Systems", *2007 International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, Aug 14-17, 2007, YiChang, HuBei, China.

[4] V.P. Kutepov, S.N. Makarievskiy, "Parallel Processes Execution Planning in Computing Systems and GRID Computing on the Base of Flowgraph Stream Parallel Programming", *2007 International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, Aug 14-17, 2007, YiChang, HuBei, China.

[5] V.P. Kutepov, V.A. Lazutkin, Liang Liu, M.A. Osipov, "The Means of Flowgraph Stream Parallel Programming for Clusters", *DCABES2006 PROCEEDING* (2006 International Symposium on Distributed Computing and Applications to Business, Engineering and Science), Oct 11-15, 2006, Hangzhou, China, Shanghai University Press, Vol.1, pp.189-194.

The Design and Application of Distributed Monitoring System Based on OPC and Wireless Communication Technology

Zhen Huang [1,2], Yongji Wang [1], Qing Liu [2]
[1]Department of Control Science and Engineering, HuaZhong University of Science and Technology
[2] School of Automation, Wuhan University of Technology
Wuhan, Hubei Province, 430063, China
Email: h-zhen@163.com, h-zhen@whut.edu.cn

ABSTRACT

Using automated control technology to speed up terminal operations is one way for raising the competition capability of the container terminal. According to the device condition of the container terminal in China, this paper first details the type of cranes and the requirement of the monitoring. Base the introduction of the OLE for Process Control (OPC) technology and the Wireless communication technology, a framework of a distributed monitoring system for container terminal crane has been put forward. The practice application results show that this system can be used in the similar container terminal in China.

Keywords: Distributed Monitoring System, Container Terminal Crane, OPC Technology, Wireless Communication Technology.

1. INTRODUCTION

Containers came into the market for international conveyance of sea freight almost five decades ago[1]. Over the recent years, the use of containers for intercontinental maritime transport has dramatically increased. Starting with 50 million twenty feet equivalent unit (TEU) in 1985, world container turnover has reached more than 350 million TEU in 2004. A further continuous increase is expected in the upcoming years, especially between Asia and Europe[2].

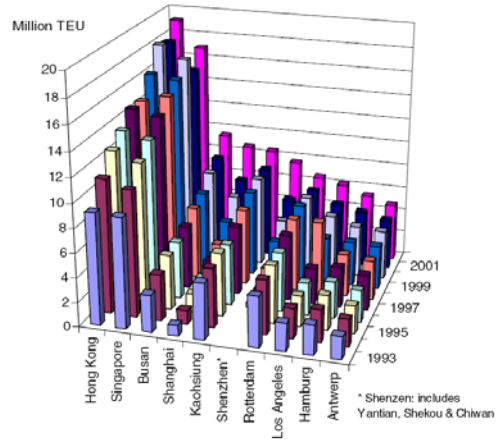


Fig.1. Container turnover of the ten largest seaport terminals in the world from 1993 to 2002(ranking 2002)[1]

Driven by huge growth rates on major maritime container routes, the competition between container terminals has considerably increased. Port authorities are looking into ways of making existing facilities more efficient. One way to improve efficiency, increase capacity, and meet future demand is to use large terminals information technology and automated control technology in order to speed up terminal operations. Then some papers about designing, analyzing, and evaluating container terminal saw a new concept – automated container terminal (ACT)[1-4]. Those container terminals called ACTs based on the use of automated guidance vehicles (AGVs), a linear motor conveyance system (LMCS), an overhead grid rail system (GR), and a high-rise automated storage and retrieval structure (AS/RS).

A detailed description of the use of these technologies in container terminals can be found in reference [5]. To use these kinds of technologies large investments have to be made and ongoing database management is required. Reference [6] show that the application of information technology in the port of Singapore results in more efficiency and a higher performance. In reference [4] it is concluded that, in order to achieve an improvement of productivity and reduction in investment costs, an advanced automated control technology is a necessary condition.

Now the discussion focuses on the China container terminals, whose efficiency and the international competition affected by the automation degree. But fortunately the ACT concept is accepted and put into practice step by step in some seaport container terminals in China, such as Shanghai, Shenzhen ports. In this paper, we design a distributed monitoring system for container terminal cranes based on the Object Linking and Embedding for Process Control (OPC) technology and the wireless communication technology. The system can be realized in most of the container terminals in China; because of the consideration equipment uses realities sufficiently.

2. CONTAINER TERMINAL CRANES

Although seaport container terminals considerably differ in size, function, and geometric layout, the principal components and the chain of the operations is the same. The chain of operations for export containers can be described as Fig.2.

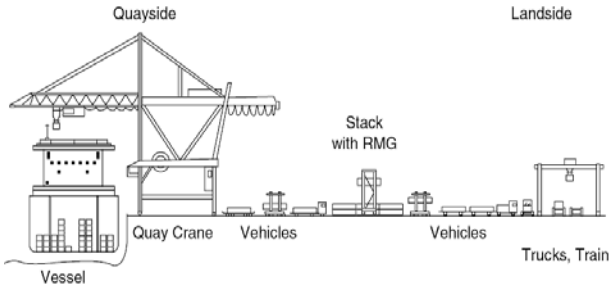


Fig.2. Transportation and handling chain of a container[1]

Usually we say that the container terminals only consist of two components: stocks and transport vehicles. The yard stacks, ships, trains, and trucks belong to the category ‘stock’, category ‘transport vehicles’ includes varied cranes and vehicles for horizontal transport. In China, the vehicles for horizontal transport almost are man-driven. In this paper cranes are the objects for the distributed monitoring system. Concerning cranes, different types are used at container

terminals.

2.1 Quay Cranes (QC)

The quay cranes for loading and unloading ships play a major role, which usually consist of five devices subsystems: the gantry, the hoist, the trolleys, the boom and the spreaders (See Fig.3).

Two types of quay cranes can be distinguished: single-trolley cranes and dual-trolley cranes. Most container terminals use the single-trolley cranes, which is man-driven. World's first post-panamac dual-trolley crane, which was designed and fabricated by ZPMC (Shanghai Zhenhua Port Machinery, China), operated at the Hamburg terminal[7]. The main trolley of the dual-trolley cranes moves the container from the ship to a platform while a second trolley picks up the container from the platform and moves it to the shore. The main trolley is man-driven while the second trolley is automatic[1]. The crane's key characteristic is its high productivity, half as much again as single-trolley crane on the same condition. At the present time, the most effective crane is the double 40' dual-trolley crane, the combination of advantages of double 40' spreaders and dual- trolley crane, is designed by ZPMC and equipment on Qingdao port, China. It can handle 80~100 boxes/h theoretically[8], while single-trolley crane's technical performance is in the range of 50~60 boxes/h[1].

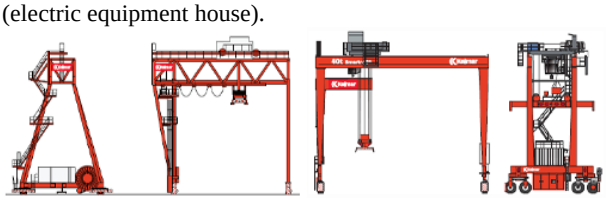
(a) Single trolley QCs (b) Dual-trolley QCs

Fig.3. Single and Dual-trolley Quay cranes

2.2 Yard Cranes (YC)

A second category of cranes is applied to stacks. The most common types of yard cranes are rail-mounted gantry (RMG) cranes, rubber-tired gantry (RTG) cranes, straddle carriers, reach stackers, and chassis-based transporters. Of these types of cranes, only RMG cranes are suited for fully automated container handling. RMG crane is often employed at one stack area along the fixed rail. To gantry wheels can turn for 90°, so that RTGs can move between different lanes, more flexible in operation, The RTG are the main yard cranes in most terminals of China.

There are two differences between the quay and the stacking crane in the framework. Firstly, the boom subsystem is only for the quay crane. When the quay crane is standby, it's often folded to avoid the collision with the big passing vessel. The second difference is the power supply. The quay crane is supplied by bank power cable; however, each RTG is powered by an AC diesel generator situated in the insulated EE-house (electric equipment house).



(a) RMG Crane (b) RTG Crane

Fig.4. The most common types of yard cranes

2.3 Cranes Monitoring Requirements and Characteristic

The higher automatic level of crane reach, the more complex the steering system is. For all types of crane, the steering systems are consisted of the programmable logic controllers (PLC). There are about 5000 varies to be monitored for a conventional quay crane and about 3000 varies for a conventional RTG. These varies can be monitored by electric engineers with a human machine interface (HMI), named as local crane monitoring system (LCMS) equipped in EE-house. Meanwhile, engineers also can supervise these varies in engineer office by the remote crane monitoring system (RCMS).

With the development of the automatic control technology and the data exchange technology, some new requirements have been put forward.

(1) Integrated. LCMS and RCMS are bundled software with the crane, so these monitoring systems are respective and only available for the cranes, purchased from same company at the same time. That increase the maintain workload of the engineer, meanwhile engineers can not supervise all cranes in one monitoring system.

(2) Mobile. LCMS and RCMS are located in the specific computer or server, so engineers can not monitor the crane working condition out of the EE-house or the engineer office.

To meet the requirements above, we design an integrated and mobile distributed monitoring system for the container terminal crane. The framework and the key technology will be discussed in detail as follow.

3. KEY TECHNOLOGYS APPLIED IN THE DISTRIBUTED MONIRORING SYSTEM FOR CONTAINER TERMINAL

3.1 OLE for Process Control (OPC) Technology

OPC was developed by the OPC Foundation, which is supported by more than 300 process-industry companies worldwide, including nearly all of the world's major providers of control systems and instrumentation. The goal of the OPC Foundation's technical committees is to develop OPC enhancements that extend its functionality, including historic data access, alarm and event message delivery, security control, and batch data access. Before the establishment of OPC standard, the industrial monitoring software engineers must take a lot of time and energy to develop varied software drivers for the devices, because each device has different industrial network and data exchange protocol. That means application software in the distributed system must be re-programmed while a bit changes had been done on the hardware. This process is usually quite complex due to the multitude of different measurement and control devices and software packages that exist in a typical industry control application[9]. Also the data accessing operation optimization is difficult to achieve for the difference between the drivers.

OPC provides a set of standard include interfaces, properties and methods for individual process monitoring and process control software to interact and share data, enabling seamless connectivity and interoperability of information between disparate industrial networks like Foundation Fieldbus, Profibus, or DeviceNet, programmable logic controller (PLC) system, a supervisory control and data acquisition system (SCADA), distributed control systems, condition monitoring, plant asset management, and production management systems[1,7,9,10].

OPC is based on Component Object Model/Distributed Component Object Model (COM/DCOM) software technology provided by Microsoft. So one OPC client application can exchange data with several OPC servers and one OPC server can supply data to several OPC clients, which are usually located in the different PCs.

OPC's evolution parallels Ethernet's move to flatten plant floor networking hierarchies[9]. As Ethernet becomes the standard for plant floor and enterprise connectivity, OPC provides a unified approach to interconnecting software solutions horizontally and vertically throughout the enterprise.

3.2 Wireless Communication Technology

It is well known that Ethernet is the dominant local area networking solution in the home and office environment. The word "Industrial Ethernet" is derived from the fact; more and more applications using communication products based on Ethernet and TCP/IP as a real-time communication vehicle in the industrial automation dominate. The dispersive automation devices and/or systems as the network node are connected by the industrial Ethernet based on the open and normalized protocol. However, there are some different voices. Reference [11] explains why conventional Ethernet is not considered as a suitable solution to support industrial communications by some people, review the new evolutions of Ethernet, and proves that new standards fill most of the requirements for an industrial solution.

Recently a large number of mobile equipments are involved in the industrial monitoring and controlling system. As described before the yard cranes are the typical large-scale moveable device in container terminal. In addition to this, chassis, reach stacker, straddle carrier, and specially the automatic guided vehicle (AGV), which nowadays plays the important role in ACT, are all belong to this type. Communication through wired for remote monitoring and controlling can cause some troubles such as cable tangling due to the movement of these equipments. Wireless Ethernet using IEEE802.11 standards provides a well-understood and well-supported means in this kind of applications. There are numerous excellent applications for wireless in the industrial domain. One of the most successful applications is wireless SCADA, where wireless is used to economically communicate across long distances in process and utility industries. Cost savings are also achieved when wireless is used to bridge communication across obstacles such as walls and rivers[12].

IEEE 802.11 is an evolving family of specifications for wireless local area networks (WLAN) developed by a working group of the institute of Electrical and Electronics Engineers (IEEE). The original 802.11 standard only supported a maximum bandwidth of 2Mbps – too slow for most applications. For this reason, IEEE expanded the standards. Nowadays most of the wireless products conform to the different wireless standards such as the 802.11a, 802.11b, 802.11g and Bluetooth, all derived from the original 802.11 standard. Table.1 lists the bandwidth and frequency of 802.11a/b/g.

Table 1. Bandwidth and Frequency of 802.11a/b/g standards

Standard	Maximum Bandwidth	Frequency
802.11a	54 Mbps	5GHz
802.11b	11 Mbps	2.4GHz
802.11g	54 Mbps	2.4GHz

At present the government has imposed strict controls over the applications of wireless LAN with 5GHz frequency in China. As view from table.1, 802.11g attempts to combine the best of both 802.11a and 802.11b, supports bandwidth up to 54Mbps and use the 2.4GHz frequency for greater range. So wireless network products conformed to 802.11b/g take the most of the wireless communication market.

4. DESIGN OF THE DISTRIBUTED MONITORING SYSTEM FOR CONTAINER TERMINAL CRANE

The distributed monitoring system for container terminal crane will be called as DMS for short in the following. The architecture of DMS based on the OPC and wireless Ethernet technology shows in Fig.5.

4.1 Framework of the DMS

Obviously, the DMS is the typical distributed system. We can see the follow characteristic.

(1) Wired/Wireless Ethernet network as the communication media of the DMS.
The cranes including QCs and YCs are distributed along the quayside or among the yard, about 10 square kilometers in the area for a large-scale terminal. As described before, the QCs usually move along the quayside fix rail, so the wired fiber optical Ethernet network can be used for data communication between the crane PLC and the data server of the DMS. But for YCs and the MPCs (mobile PC browsing terminals), the wireless Ethernet network will be chosen.

(2) A uniform and openness data exchange interface based on the OPC technology.
There are usually different series of PLC controller used on the crane control system, including GE Series 9030, YASKAWA CP-316 and CP-317, Fuji F120S and F70S, ABB AC800M, and so on. DMS must supply an integrated solution for the data exchange between the DMS and the PLC controllers. Fortunately, the manufacturers of the PLC mentioned above are all the member of the OPC Foundation, and can offer the communication modules supported Ethernet. Therefore, the OPC-DA based on Ethernet will be used to solve this problem. All the devices or subsystems supporting OPC technology can be the objects of the DMS easily, which ensure the system's expansibility.

(3) Layering and distributed Function architecture.
The whole architecture can be divided to three layers according to the function: device layer, database layer, monitoring application layer. In device layer, the PLC control system of crane achieves the real-time control and fault handling function independently, in the mean time supplies the real-time data to data server. Database servers transform the device information to the uniform OPC data source shared between the application computers in the upper layer. The end-user just faces the function applied by application layer.

4.2 Software Configuration of the DMS

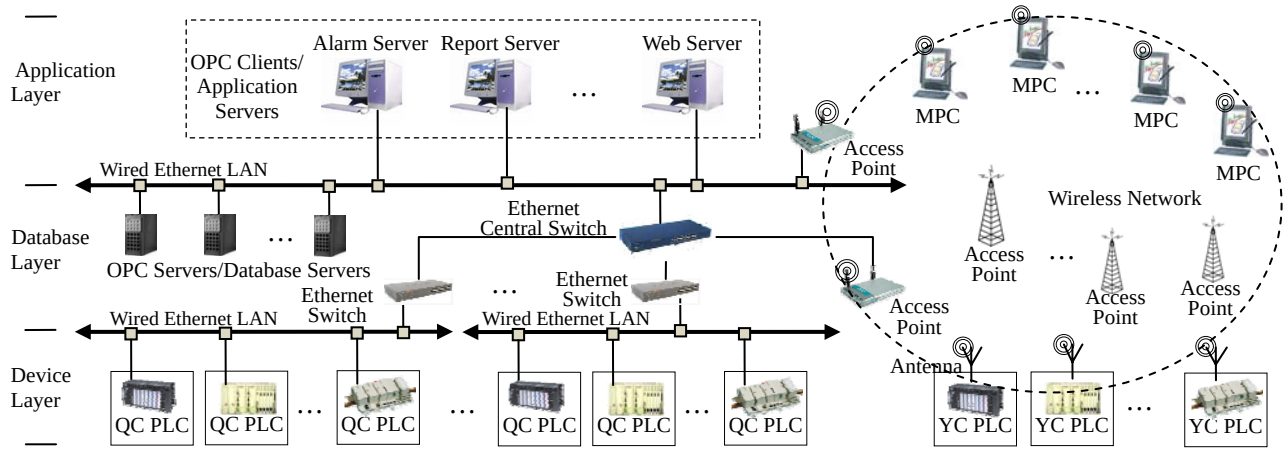


Fig. 5. The framework of distributed monitoring system based on OPC and Wireless Ethernet

Hardware for distributed systems is important, but it is software that largely determines what a distributed system actually looks. First, they act as resource managers for the underlying hardware, allowing multiple users and applications to share resources such as CPUs, memories, peripheral devices, the network, and data of all kinds. Second, and perhaps more important, is that distributed systems attempt to hide the intricacies and heterogeneous nature of the underlying hardware by providing a virtual machine on which applications can be easily executed[13].

The OPC server software applied by the manufacturers of the PLC control systems will be installed in database servers. Nowadays, there is some special OPC server software such as KEPServerEx, which let us use the OPC client application to collect data from the device nonsupport OPC. To balance the load of the data gathering, the number and data gathering scale of database server can be set according to the model of the PLC controller, geographical position or data size.

The application software design tool can choose the industrial configuration software, which is the SCADA toolkit for the PC platform, such as WinCC (Siemens) , FIX (Intellution) , Intouch (WonderWare), RSView32 (Rockwell Automation) and so on. As the development of the OPC technology, most of the configuration software supports the OPC standard protocol. As the configurations of the multi-client/multi-server, the application function such as statue monitoring, alarming, reporting can be distributed in the system.

4.3 Functions of the DMS

The functions of the DMS are described as follow:

(1) Remote monitoring. DMS can directly access and browse QC and YC PLCs for cranes condition monitoring, fault diagnostic, hour meters, counters record and more. Engineers can supervise all cranes in one system because of the integrated and openness interface.

(2) Remote online PLC programming. DMS allows the authorized engineers browsing the PLC ladder diagram for cranes real-time condition, and modifying the programs online.

(3) Mobile Browsing. It is using mobile browsing terminals such as mobile PC that engineers can browse condition and program of the appointed crane at the same time wherever within the wireless signal cover.

5. CASE STUDY

The design has been applied to a large-scale container terminal in south of China. The DMS takes full advantage of the exiting network resource in that container terminal.

- 100 Base-FX Fiber Optical Network for data communication of quay cranes.
- Wireless Network using IEEE802.b (frequency band of 2.4~2.4835GHz) for data communication of yard cranes. The wireless network consists of over 40 Access Points (AP) and 70 sets of directional Antenna, covering all Operational Area within the container terminal.

The designed maximum monitoring range is 38 YCs and 154 QCs, including 12 MPCs. The different series of PLC controller mentioned in chapter 4 all involve in this case. The MPC accesses the web server in Browser/Server mode, which asks no other requirement for the MPC except the IE browser. It is impossible that all cranes work at the same time in practice application. For 20 working cranes, the data refresh rate in the HMI is about one to two seconds. Because the data refresh rate is mainly influenced by wireless network bandwidth, and the data request in MPC is windows mode, so the refresh rate will not exponential increase with the increase of the working cranes.

The DMS shares the wireless network, which has the maximum 11Mbps bandwidth and only 1Mbps bandwidth while the signal near the ground, with RTG dispatching system. Therefore, the wireless signal of the MPC is not good or even zero in some place within the container terminal. To improve the performance of the DMS, an unshared wireless network must be set up.

6. CONCLUSIONS

This paper proposes a framework of the distributed monitoring system for container terminal crane. The result of the practice application proves that this DMS can be used in most of the similar container terminal in China, to raise the automatic lever.

The study object of this design is limited to the cranes. With the development of the port, more and more device such as the horizontal transportation vehicles will become the object of the automation system. The further study will be focus on the optimization of the network and the architecture to cover more devices.

The field of remote control of industrial equipment which needs precise control has still many problems to solve such as real-time control or restoration of load loss. With the development of the network technology, the distributed monitoring and remote control system, which is the further research subject, will take an important role in ACT.

REFERENCES

[1] Steenken, D., Voss, S. and Stahlbock, R., "Container terminal operation and operations research - a classification and literature review", *Or Spectrum*, Vol.26, No.1, Jan2004, pp.3-49.

[2] Gunther, H.O. and Kim, K.H., "Container terminals and terminal operations", *Or Spectrum*, Vol.28, No.4, Oct2006, pp.437-445.

[3] Liu, C.I., Jula, H. and Ioannou, P.A., "Design, simulation, and evaluation of automated container terminals", I*EEE Transactions on Intelligent Transportation Systems*, Vol.3, No.1, Mar2002, pp. 12-26.

[4] Leeper, J., "Integrated automated terminal operations", *Transportation Research Circular*, Vol. 33, 1988, pp. 23-28.

[5] RS, J., "Gate solutions", Paper presented at the *Container port and Terminal Performance Conference*, Amsterdam, 1999.

[6] Wan TB, W.E., Meng LC, "The use of information technology by the port of Singapore authority", *World Development* Vol.20, No.12, 1992, pp.1785-1795.

[7] OPC, F., "OPC Historical Data Access Automation Interface Standard, v1.0", Jan 6, 2001.

[8] Fernandez, A.F., Rodeghiero, P., Brichard, B. et al., "Radiation-tolerant Raman distributed temperature monitoring system for large nuclear infrastructures", *IEEE Transactions on Nuclear Science*, Vol.52, No.6, Dec2005, pp.2689-2694.

[9] Holley, D.W., "Understanding and using OPC for maintenance and reliability applications", Computing & Control Engineering Journal, Vol.15, No.1, Feb-Mar2004, pp.28-31.

[10] Liu, J., Lim, K.W., Ho, W.K. et al., "Using the OPC standard for real-time process monitoring and control", *IEEE Software*, Vol.22, No.6, Nov-Dec2005, pp.54-59.

[11] Decotignie, J.D., "Ethernet-based real-time and industrial communications", *Proceedings of the IEEE*, Vol.93, No.6, Jun 2005, pp.1102-1117.

[12] Piggin, R. and Brandt, D., "Wireless Ethernet for industrial applications", *Assembly Automation*, Vol.26, No.3, 2006, pp.205-215.

[13] Tanenbaum, A.S. and Steen, M.v. Distributed Systems: Principles and Paradigms, New York: Prentice Hall; US Ed edition 2002.

[14] Kim, J.Y., "A TCP/IP-based remote control system for yard cranes in a port container terminal", Robotica, Vol.24, Sep-Oct 2006, pp.613-620.

[15] Kapsalis, V., Koubias, S. and Papadopoulos, G., "OPC-SMS: a wireless gateway to OPC-based data sources", *Computer Standards & Interfaces*, Vol.24, No.5, Nov 2002, pp.437-451.

Zhen Huang received her B.Sc. degree in Electric Automation at Wuhan Transportation University in 1996 and her M.Sc. degree in Control Theory and Control Engineering at Wuhan Transportation University in 1999. She is a Ph.D candidate at Huazhong University of Technology and Science. Her research interests include intelligent system, neural networks, fuzzy logic control, and real-time control systems.

Qing Liu received her B.Sc. degree in Electric Automation at Wuhan Water Transportation Engineering Institute in 1985, and her M.Sc. degree in Electric Drive & Automation at Wuhan Transportation University in 1988, and her Ph.D. degree in Ship steering and Control at the Wuhan University of Technology in 2002, in China. Dr. Liu is currently a Professor of Electric Engineering and Automation at the Wuhan University of Technology in Wuhan, China. Her research interests include intelligent system, neural networks, fuzzy logic control, mobile robotics, and real-time control systems.

Analysis of CSTN's Model and Special Transportation Solution

Liyi Zhang, Shitong Zhang, Min Xu
Center for Studies of Information Resources, Wuhan University
Wuhan, Hubei, 430072, China
Email: lyzhang@whu.edu.cn

ABSTRACT

With the development of social economy, special transportation has been becoming more and more important in China. Many websites have integrated special transportation services as a key part of logistics services. But there are still many problems in China's special transportation services. This paper firstly presents the model and key ideas of China Special Transportation Network (CSTN) and then analyzes its All-way Solution of special transportation. Finally, it describes the design of the SMS platform system and identity authentication system.

Keywords: Special Transportation, hina Special Transportation Network, All-way Solution Project, SMS platform, EJBCA

1. INTRODUCTION

The so-called special transportations refer to the transportations which need special carriers and schemes. The most outstanding character of the special transportation is that whether the technical parameters of the transport carriers in the special transportation can satisfy the transport demands of some particular products. The fields of the special transportation are between the comprehensive fields of the general logistics services network (such as Jincheng Logistics network) and the specialized fields of the special transportation services network (such as China Refrigeration Network). Therefore it should focus on the services in the mid-fields. Special transportation services should reference the comprehensive nature of the general logistics services and meanwhile learn from the specialty of a special transportation network. Basing on the special transportation services, we should summarize the commonness of all kind of special transportations. Finally, we can provide a comprehensive and integrated transportation services for the special transportation[1-3].

2. THE MODEL OF CHINA SPECIAL TRANSPORT NETWORK

The China Special Transportation Network (CSTN-www.teyun.com.cn) was founded in 2006, and its key idea is the all-way solution for transportation enterprises and vehicles in the special transportation industry. The all-way solution project of CSTN is created to ensure that both the owners of the vehicles and the goods will get the maximal income in a safer and more effective way at the lowest cost. It provides concrete settling projects such as loading, discharging, option of the route, road condition on the way, local transport regulation, necessary procedure of commission during the executing process of the special transportation after the signature of the contract. It depends on the service insiders on the net platform to implement the concrete services.

Besides the all-way solution, CSTN also provides security and cooperation. The cooperation is the mutual cooperation among all departments and related interests owners, but not only the cooperation between the consigner and the carrier. Through such kind of all-round cooperation, an all-way solution project will be provided to the special transportation.

2.1 The All-way Solution Project in CSTN

The all-way solution project of CSTN includes: value-added services and the assistant equipments, information consultation of the road condition on the way; process of the special transportation licenses, vehicle inspection and repair on the way and timely response to the emergency.

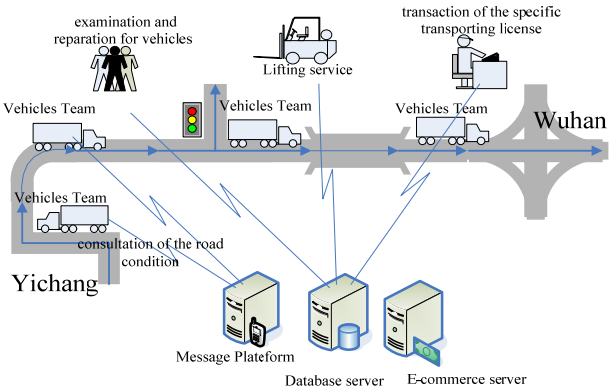


Fig. 1. Schematic map of all-way solution project

1) Value-added services and the assistant equipments.
CSTN combines the local specialized companies which provide services such as suspending, installing, and lifting and the assistant equipments as their assistant members in each pivotal city where there are much loading and unloading activities. They will provide the vehicles on the way with cheaper and more specialized value-added services to safeguard the special transportation vehicles.

2) Information consultation of the road condition on the way.
CSTN takes two methods to provide drivers with information consultation of the road condition on the way. Firstly, CSTN employs special information researchers majoring in investigating the road condition on the way in a certain period and then the summarized useful information is stored in the system database. Secondly, CSTN has many network members, and they can provide CSTN with the summarized information about the road condition of the transport route after they finish a special transportation and the information will also be stored in the system database. By this way, when there is transportation task on the repeated route CSTN will firstly pick out the summarized information and give it to the vehicle drivers. With the help of the road condition system database, CSTN can ensure its members of the timely and correct information of road condition on the way.

3) Process of the special transport license.
Because the particularity of the transportation of the special goods such as bulk cargos, dangerous materials, etc. it requires applying for many transport licenses, and the process of application is complex. CSTN entrusts some local

members with processing the licenses for the special transport vehicles ahead of time in every place where transport license needs to be applied. By this way, the vehicles of a special transportation can cross each city smoothly.

4) The inspection and repair for vehicles on the way.
To be safely, CSTN can provide vehicle drivers with the contacting means with its motor repair members. When vehicles need inspection or repair in some place, drivers may not go purposelessly to find a vehicle maintaining station in a strange place. They just need to dial the number of the members which CSTN gives them. And they will come to give vehicles a careful examination and repair and make your vehicles resume in time so that you can start off and complete you task successfully.

5) Timely response to the emergency.
Though CSTN can provide four functional modes above, and can avoid problems during the transportation maximally. However, not all things are under consideration. Therefore, CSTN also provides the 24-hour timely response hot-line to deal with the emergency during the transportation. When paroxysmal matters happen during the transport process, CSTN will find the solution as soon as the phone is dialed.

2.2 Other Value-added Services

CSTN also provides other value-added services, for example: industry consultation, inquiry of the cell phone's ascription place, inquiry of China area code, inquiry of the mileage and so on. Trade consultation provides the latest trends, law and regulation, news and reports about the special transport industry, which are the basis for special transport industry to make long term tactics. The data for the inquiry of the mileage come from national main trunk mileage data. We use XML to create dynamic data sets and timely updates. Finally, we find the shortest highway route through a shortest path algorithm and the result will be several programs. Integrating the programs with real-time traffic situation, users can choose the best transport program.

Considering the particularity of the users of the website, it is inconvenient for the drivers in the way to go online, so CSTN provides its members with convenient message platform. A small cell phone can be used to send the information of the vehicle, the goods, the request of the identity authentication, information about the vehicles online, request of inquiring the road condition and so on. For example, when the vehicle is empty and goods need to be given, information of such demands can be send as following.

The format for cell phone to send message: A#B#C

Here, A means whether the vehicle is empty, when it has goods, 1 is input, otherwise, 0 is input.

B refers to the location of the vehicle at present, and it is expressed by the area code or zip code

3. COMBINATION BETWEEN CSTN AND MOBILE COMMERCE

The internet can be connected with the SMS Network in three ways.
The first approach is that the internet cooperates with the mobile service operators (SO) directly, and gets a special-service numbers. Besides, we pay for the services according to a certain accounting method and can acquire some technical support from the mobile SO. This approach often has high stability and quality. However, the related costs are high. Moreover, a relatively high threshold may be set up by the mobile service operator. A SP usually adopt this approach to connect with the mobile service operators.

And the second approach is to connect with the mobile SO with the help of the SP. That is the internet being connected to mobile service operators with the SP as an intermediary. A SP can provide accesses for more than 100 users. It is bound to affect the communicating quality and the stability must be affected by the SP itself.

The final approach is connecting with the mobile SO with the help of their own SMS modem which supports GSM (Global System for Mobile Communications). With an SMS modem and a mobile phone SIM card, we can send and receive text messages like using a common mobile phone and needn't any other procedures. Comparing with the above two approaches, this one is more convenient and its stability is relatively higher. The only disadvantage is the limited transmission capacity and speed.

Here, we use equipment named SMS Modem which supports GSM. It can get access to the SMS gateway which is a component of SMS server center through a wireless access. [7]

Considering that CSTN's requirement is not too high and is usually stable, we choose the third one as the approach to access to the SMS network in our CSTN's SMS Platform System.

3.1 The Framework of CSTN's SMS Platform

As Fig 2 shows that the framework of CSTN's SMS platform is composed by three tiers: R/S (Receive /Send) Protocol Control Tier, R/S Control Tier and Application Tier. The R/S Protocol Control Tier is responsible for using some SMPP Message gateway protocol such as CMPP, SGIP, SMGP, SMPP and producing a platform-crossed SMS service. So it can provide a SMS R/S interface for the above Tiers. Here we use the JSMSEngine 2.0.4, which is a popular open-source java package in the internet. The R/S Control Tier is responsible for packaging the messages which need to be sent and unpacking the received SMS formatted text messages from the SMS server centers and routing and choosing an appropriate application for the received messages. Text message package is to package the text messages which include the Cell Phone Numbers, Text Message, SMS Gateway Protocol, SMS Encoding, etc in accordance with the requirements of the R/S interface format and then send them to the R/S Protocol Control Tier whose duty is to send the text message to the SMS server center. The third Tier – the Application Tier has to analyze the messages and then choose a certain application unit to deal with and respond to them. The Application Tier is mainly dealing with the content of the text message and the operation of receiving and the sending of the text message means a black-box to the Application Tier[6].

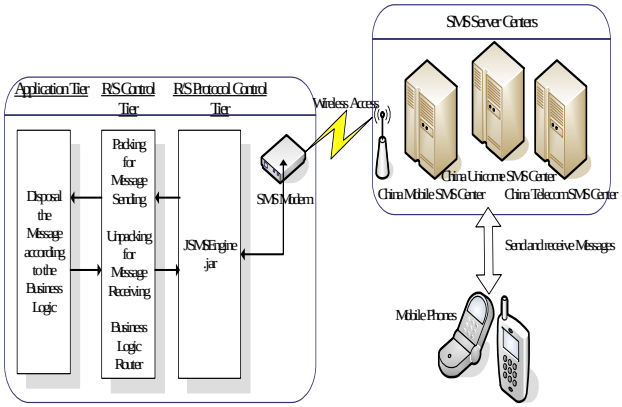


Fig. 2. The framework of CSTN's SMS platform

3.2 The Design of R/S Control Tier

R/S Control Tier has three tasks: sending text messages, receiving text messages and application routing. Moreover, necessary log document must be written in. Sending and receiving text messages are both communicating operations, while the writing of log is a database operation and the application routing is a web operation. Three independent threads are designed to take charges of these three functional operations. And we have also set two text-message queues to manager the text messages. The structure of R/S Control Tier is shown as Fig 3.

R/S Control Tier is a gateway communication tier which takes responsibility to maintain a connection to the gateway, send messages to the gateway, and receive messages from the gateway and send them to Message Receiver Queue.

Message Sender Queue and Message Receiver Queue are two queues which see to the message management.

Application Router takes responsibility to send text messages to the related application.

Logger Thread is a log-writing program which fetchs text messages from the message queues, and then write in the log.

Sender Thread is a thread program which submits text messages to R/S Control Tier. The SMS gateway protocol is asynchronous, however, in most of the time, a synchronous one is needed which means that we have to know whether the sending is successful. Therefore, Sender Thread always provides a method to keep synchronous. After sending a text message, Sender Thread will waite for the result until it is notice that the message has been sended sucessfully or not.
Receiver Thread is a thread program which sees to receive the text messages. It fetches the text messages from Message Reciever Queue and then delivers them to different application routers according to the contents of the text messages[7][9].

The data structure of text message class and the queue algorithm are described as follows. The queue is designed as a linked list which uses "lastNode" as a reference variable. [8]

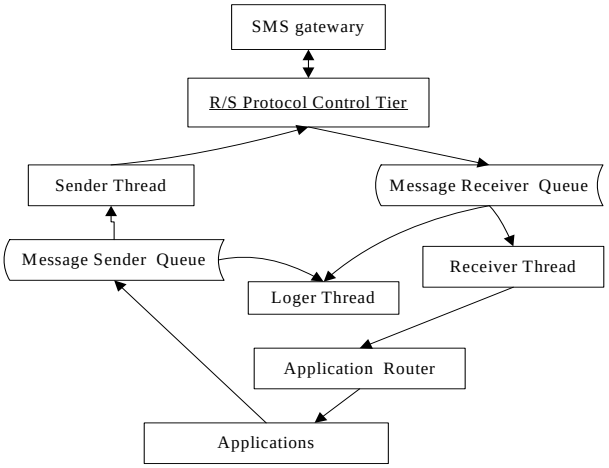


Fig. 3. Structure of the R/S Control Tier

```
class MessageBean{
   //definition of MessageBean
   private String cellPhoneNumbers;
   private String textMessage;
   public MessageBean(String cellPhoneNumbers, String
textMessage){
        this.cellPhoneNumbers = cellPhoneNumbers;
        this.textMessage = textMessage;
   }
  //get and set methods
   } //end class MessageBean
class Node{
//definition of a Node
   private MessageBean item;
   private Node nextNode;
   public Node(MessageBean mewItem){
        item = newItem;
        nextNode=null;
   }
  public Node(MessageBean mewItem,Node next){
        item = newItem;
        nextNode=next;
   }
  //get and set methods
 } //end class Node
 public class MessageQueue{
  //definition of MessageQueue
  private Node lastNode;
  public MessageQueue(){
  lastNode=null;
  } //end structure method MessageQueue
  public isEmpty(){
   //determines whether a queue is empty
   return lastNode==null; }
  public enqueque(MessageBean newMessage){
  //insert a new node
   } //end enqueque
 public MessageBean dequeque throws QueueException(){
  //retrives and removes the front of the queue
 } //end dequeue
 public MessageBean peek throws QueueException(){
 // retrives the item at the front of the queue
 } //end peek
 } //end class MessageQueue
```

4. THE IDENTITY AUTHENTICATION SOLUTION OF CSTN

The identity authentication of CSTN includes: individual authentication, enterprise authentication, vehicle authentication, and driver authentication combining with position authentication and authorization authentication.

CSTN takes EJBCA authentication system as reference, and has created its own identity authentication system which combines its own unique special transport authentication system and the third-party certification institutions. And relying on the SMS text message platform, the function of the SMS authentication is added. The third-party certification is shown as follows.

CSTN takes the identity authentication mode of www.56110.cn as reference, and combined with the NCIIS (National Citizen Identity Information System). The NCIIS, which is developed by the Ministry of Public Security of China, provides the information which is needed to check the individual certificate of the CSTN. Besides, the NCIIS also provides the enterprises with checking services. The result of the identity check is the name and ID numbers provided by the NCIIS through CSTN. The system compares the data offered by the checker with the data stored, and returns the result to the checker. The result only includes whether the comparison is consistent or not but doesn't provide the user with other information of the checker except the photos. Thereby, this individual identity authentication system doesn't involve in violating the citizens' personal privacy[3].

Enterprise authentication of CSTN is cooperated with SAIC (State Administration for Industry & Commerce of China) and SAT (State Administration of Taxation). The business license of the enterprises and the tax registration certificates will be checked by the authentication system of the two state administrations. The applicant of the enterprise member must pass the individual identity authentication. The enterprise members need to validate the information of the enterprise as well as the following information:

(1) Whether the data of the enterprise is registered in the SAIC.
(2) Whether the position and status of the applicant in the enterprise are true.
(3) Whether the application is with the enterprise's permission

The driver's driving certificate and the steering certificate of the vehicle must be validated during the process of the authentication of the vehicle. If necessary, some special certificates of the vehicles are asked to be handed in.

The authentication of the driver is conducted by the driver's driving certificate, the steering certificate of the vehicle as well as the driver's individual identity authentication

EJBCA is an enterprise class Certificate Authority using J2EE technology. EJBCA depends on the J2EE platform to constitute a robust, high performance and component based CA. Both flexible and platform independent, EJBCA can be used standalone or integrated in any J2EE application[4][5].

J2EE use multi-Tier distributed application model. These models are divided into several functional components. These Tiers include client tier, web tier, business tier and data tier. Business tier is also named EJB tier in EJBCA, which contains two major components——RA component and CA component[4][5].

However, in order to achieve the requirement of the third-party authentication and the text message authentication. We should restructure the framework of EJBCA as Fig 3 shows. The Web Tier is rebuilt and transformed to WEB/Mobile Tier into which the Mobile Container is added, and the Mobile Container contains SMS component. A third party authentication component is added into the RA component. When the user registers using RA, his registration can success only after the registration information being certificated by the third-party and then the information will be added into the local database.

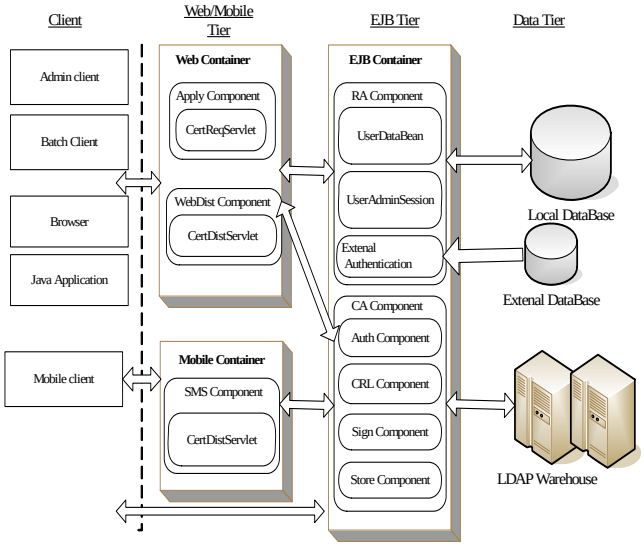


Fig. 4. The framework of CSTN's authentication system

5. CONCLUSIONS

Combining various logistics website examples, taking the experiences of a number of special transport website, the all-way solution proposed by CSTN provides all-round services such as information platform, information consultation and so on. It has made a great progress in special transport services avoiding single service. Especially, the design of the SMS platform system and identity authentication system is another innovative exploration in the field of special transport services.

REFERENCES

[1] The Overall Situation of China's logistics Market in the"11th Five-Year Plan" Period. China Network. http://www.china.com.cn/China/EC-c/. 2006/12/20.
[2] China Cargo Logistics Information Platform. http://www.56110.cn. 2006/12/20.
[3] Jin Cheng Logistics Network. http://www.jctrans.com. 2006/06/13.
[4] Ejbca-Design. http://sourceforge.net/project/showfiles.php?group_id=39716. 2007/3/20.
[5] Zhou Bishui, Zhang Lei. "Research of EJBCA on WPKI Environment". *Computer Engineering and Design*. 2005 (8).
[6] Enterprise Text Message Platform. www.jrsoft.com.cn/Product/Aviation/sms.asp 2007/03/20
[7] The SMS Interface Platform. http://zeroliu.blogdriver.com/zeroliu/1215155.html. 2007/04/10.
[8] Frank M.Carrano and Janet J.Prichard. *Data Abstraction and Problem Solving with java*. 217~220. Tsinghua University Press. 2004.

[9] Zhu Qi. "Web-Oriented JMS Application Systems". *Computer Engineering and Design*. 2005 (11).
[10] Chen Qin, Ling Qingsheng. "Research On Security CA-EJBCA", Computer Engineering and Design,. 2005 (12).

Liyi Zhang is a professor and dean of Department of Information & E_commerce in School of Information Management, Wuhan University. He graduated from Wuhan University of Hydraulic & Electric Engineering in 1988; from Xi'an jiaotong University in 1991 with specialty of Pattern Recognition & AI; from Wuhan University in 1999 with specialty of System Engineering. He is a member of E_commerce Major Guiding Committee of China, is Secretary-general of Association of Hubei Electronic Commerce, and a member of AIS(Association of Information System). He has published five books, over 40 Journal papers. His research interests include information system, e-commerce and information retrieval.

Semantic Based Virtual Organization Model

Wang Chu, Depei Qian
Department of Computer Science and Technology, Xi'an Jiaotong University
Xi'an, Shaanxi 710049, China
Email: sdchuw@163.com

ABSTRACT

Virtual organization has emerged as important research field. But less attention is paid to the semantic based model of virtual organizations, virtual organizations creation and evolution are still difficult. This paper combines semantic web technology with architecture based modeling approach to semantically describe virtual organizations and yield semantic based virtual organization model. Component specification is attached with semantic information and component relationships are semantically defined. The semantic based virtual organization model supports semantic match between business requirements and semantic Grid services. The semantic of relationships and entities are defined rigorously, a primary benefit is that they facilitate automated reasoning. Patterns are used to describe business component composition and service component composition, and support virtual organization integration at varying levels of granularity. Patterns map business goal into Grid services so that virtual organization evolution is supported effectively.

Keywords: Grid Computing, Virtual Organizations, Architecture Based Modeling, Semantic Based Model, Composition Pattern

1. INTRODUCTION

Turbulent market conditions characterized by very fast and continuous changes are forcing enterprises to adopt new organizational and production paradigms. Enterprises need a way of building, delivering, and orchestrating IT resources. This trend is facilitated by the advances in Web services and Grid computing. Virtual organizations are major trend in cooperative business [1, 2].

Although the advantages of the virtual organizations are well known at the conceptual level, but most researches focus on the interoperability of Grid services and semantic Grid, little effort is put on the semantic based model of virtual organizations. Virtual organizations creation, management, and evolution are still difficult [3]. There are many research challenges behind virtual organizations:

1) *Semantic based virtual organization model*: One important aspect in virtual organizations application is the specification of the organization model [4]. The purpose of such a model is to specify resources management, task allocation, and to support virtual organizations management that aims at monitoring of operations on a business process level and automatically mapping high-level business goal to the actual Grid services. Another key aspect is to maintain global coherence of virtual organizations. This calls for a means to pool business knowledge, determine shared goals, determine common tasks across services, and avoid conflicts [5].The discovery of a service means that a published Grid service matches the virtual organization's requirements. Existing researches focus on semantic description of Grid services, but the virtual organization's requirements lack semantic information. It is difficult to satisfy the need for semantic matching [6].
2) *Evolution management*: To facilitate virtual organizations evolution, the traceability between business goal and Grid services should be maintained [7]. Currently, in the process of virtual organization creation, business knowledge is frequently tacit, embedded in practice and experience rather than explicitly modeled, which makes sharing and adaptation extremely difficult. Thus, it is impossible to use machine reasoning in order to identify potential side effects of modifications. Also, process improvement should be conducted for global process optimum, however, this cannot be achieved without a proper architecture of virtual organization [1, 8].

This paper combines semantic Web technology with architecture based modeling approach to semantically describe the component and the component relationships of virtual organizations explicitly, to prepare necessary control structure for the formed virtual organization. Architecture describes the acceptable pattern of component composition and supports dynamic evolution required for agility and reconfigurability. Architecture based modeling approach is a good approach to support tackling the inherent complexity of virtual organizations [9,10]. In this paper, the term 'semantic' denotes the semantic specification of the business component and Web/Grid service component and the semantic definition of component relationships.

This paper is organized as follows. Section 2 outlines the related work on virtual organizations research. Section 3 details the semantic based model of virtual organizations. Section 4 depicts an example of virtual organization. Finally, section 5 rounds up the paper with conclusions.

2. RELATED WORK

Randy Howard et al. introduce a framework that addresses the following issues: 1) transaction control and workflow management; and 2) resource management and evolution of the Virtual Enterprise. The framework facilitates management, coordination, and interoperability for the loosely-coupled, distributed, and diverse services. The framework presumes that the virtual organization has more visibility into the partners' environments than with ordinary Web services, thus allowing the additional knowledge to optimize the interactions through Web services [11].

Shalil Majithia et al. present an architecture to facilitate automated discovery, selection, and composition of Semantic Grid services. They distinguish between different levels of abstraction of loosely coupled workflows to facilitate reuse and sharing, and allow users to specify and dynamically refine a high-level objective of the virtual organization that is then translated into a workflow. It is possible to carry out "what-if" analysis in an efficient manner when some sub-processes are changed [12].

Business Process Management (BPM) is an approach to manage the execution of IT-supported business operations. However, BPM does not provide a uniform representation of an organization's process space on a semantic level, the degree of mechanization in BPM is still very limited, creating inertia in the necessary evolution and dynamics of business processes. Martin Hepp et al. propose to combine Semantic Web and BPM and yield one consolidated technology that is called Semantic Business Process Management, which supports both agile process implementation and querying the business process space by logical expressions [8].

Aniruddha Gokhale et al. apply model-driven approach to assemble and deploy Grid applications. They describe Grid component based on the Object Management Group's (OMG) CORBA Component Model (CCM), UML is used to model Grid application requirements, and expose the deployed Grid component as a Web service that enables Grid applications to use ubiquitous web protocols to create, join, or leave collaborative Grid applications [13].

3. ARCHITECTURE BASED VIRTUAL ORGANIZATION MODELING

3.1 Architecture Based Modeling Approach

The Architecture based modeling approach follows the "divide-and-conquer" method of defining architecture that consists of three activities: goal decomposing, architecture defining, and validating.

1) goal decomposing: the objective of this activity is to divide the system goal into a number of sub-goals and assign them to components. In this activity, "Responsibility-Assignment" relationships between system goal and components are created, and they are called γ-relationships in this paper.
2) architecture defining: the objective of this activity is to construct architecture to achieve the system goal. Determining choreography of the components is the major work of this activity. "Take-Part-In" relationships between component and architecture are created, and they are called β-relationships. Assembly by choreography is a technique that makes virtual organizations creation much easier [10, 14].
3) validating: the objective of this activity is to check whether the constructed architecture meets the system goal. In this activity, "Achieved-By" relationship between the system goal and the architecture is created, and it is called λ-relationship.

The divide-and-conquer procedure results in a pattern, written as $L\rightarrow_{\lambda}A\{C_i|i\in N\}$, which contains following component relationships: $\{\gamma_i: L\rightarrow C_i|i\in N\}$, $\{\beta_i: C_i\rightarrow A|i\in N\}$, and $\lambda: L\rightarrow A$, where L, C, and A represent "Goal/requirements", "Component", and "Architecture" respectively.

A pattern is an abstraction that is aimed to be automatically transformed into final artifact, like Java source code, that can be used in implementation. This means that patterns are not just documentation, that can be used as help in the design process. There has been considerable researches on identifying relevant patterns for different application areas. The Grid community has also recognized the importance of patterns as a way to reuse expert knowledge. Patterns are not just a modeling abstraction, but have also been included into development tools as first class entities. Furthermore, application reusability and maintenance is improved if patterns are still identifiable in the final code. Component paradigms also provide patterns as first class entities, where patterns may be defined, stored and reused independently of the components [15].

3.2 Role and Business Model

Workflows need to work within a structure of organization and local constraints. Virtual organizations need to perceive the condition of the environment and actions accordingly, and need to be more adaptive by providing a structure. It is a natural way to conceptualize organization as roles and relationships. A role is a business component that is situated in some environment and capable of flexible, autonomous action in that environment in order to meet its business goal [16].

We use the concept of role as a means to encapsulate the business goal, constituent partners, activities, and constrains. Roles are: (1) clearly identifiable business entities with well-defined boundaries and interfaces; (2) situated in a particular environment—they receive inputs related to the state of their environment, access resources, and act on the environment; (3) designed to fulfill specific business goals; (4) autonomous— they have control both over their internal state and over their own behavior; (5) capable of constructing hierarchical structure. Roles can serve as building blocks to construct complex virtual organizations on the basis of integration and extension.

Definition 3.1 (Organization pattern) Let R_0, $\{R_i|i\in N\}$, and R be roles, R_0 only contains business goal, and there exist $\{\gamma_i: R_0\rightarrow R_i|i\in N\}$ and $\{\beta_i: R_i\rightarrow R|i\in N\}$. If there exists $\lambda: R_0\rightarrow R$ then R_0, R, $\{R_i\}$, $\{\gamma_i\}$, $\{\beta_i\}$, and λ constitute an organization pattern, written as $R_0\rightarrow_{\lambda}R\{R_i|i\in N\}$.

Organization patterns are specified at several levels of functionality or granularity in a consistent way and can be used to describe virtual department, virtual team, or whole virtual organization.

Definition 3.2 (Business model) A business model is a set of organization patterns at different levels of granularity, written as $B_M=\{R_0^j\rightarrow_{\lambda j}R^j\{R_i|i\in N\}|\ j\leq n\}$, where n is the number of the organization patterns.

Business architecture can be dynamically evolved when volatile business rules change or new cross organizational links come into force, while ensuring compliance to core business invariants.

3.3 Service Component and Service Model

Most service composition approaches attempt to address service composition by composing single web services from scratch, ignoring reuse of existing compositions. From a developer's perspective the higher level of service integration will lead to more efficient, more structured composition process that will accelerate application development [17].We use the service component to encapsulate the common goals (functional and nonfunctional goals), operations, constituent services, behavior, and choreography. Service component is a packaging mechanism combining published web services, it has a recursive nature in that it is composed of published web services while in turn it is also considered to be itself web service.

Definition 3.3 (Service composition pattern) Let G_0, $\{G_i|i\in N\}$,

and G be service components, G_0 only contains requirements, and there exist $\{\gamma_i: G_0 \rightarrow G_i | i \in N\}$ and $\{\beta_i: G_i \rightarrow G | i \in N\}$. If there exists λ: $G_0 \rightarrow G$ then G_0, G, $\{G_i\}$, $\{\gamma_i\}$, $\{\beta_i\}$, and λ constitute a service composition pattern, written as $G_0 \rightarrow_\lambda G\{G_i | i \in N\}$.
Service composition pattern offers an adequate means to deal with the granularity variation problem.

Definition 3.4 (Service model) A service model is a set of service composition patterns at different abstract levels, written as $S_M=\{G_0^k \rightarrow_{\lambda k} G^k\{G_i | i \in N\} | k \leq m\}$, where m is the number of the patterns.

Service composition patterns describe how to compose existing services and provide a seamless record of trace information from high-level requirements down to simple services.

3.4 Semantic Based Virtual Organization Model
In this paper, component specifications with semantic information are used to describe roles in business world and services in Grid environment. First of all, we discuss the component specification.

A component specification provides domain-specific information and includes following parts: *Category*, *Global-goal*, *Constituent Partners*, *Operations*, *Resources*, *Choreography*, and *Behavior*.

Category contains five attributes: *ID*, *Domain*, *Name*, *Synonyms*, and *Abbreviations*. The *ID* attribute is unique component identifier that takes the form of a Universally Unique ID. *Domain* gives the area of interest of the component. The *Synonyms* attribute contains a set of alternative characteristics of *Name*. The *Abbreviations* attribute is a set of short forms of *Name*. Components take part in an architecture (composite component) through their *Operations*. *Global-goal* (including functional goal and non-functional goal) gives the reason for existence of the component. *Constituent Partners* are components that cooperate with each other and regulated by *Choreography*.

Operations are described at four levels: *syntactic*, *semantic*, *operational*, and *registered service*.

Syntactic properties: *Operations* are syntactically described by the following attributes: *Op-ID*, *name*, *mode*, *input*, and *output*. The *Op-ID* attribute is unique operation identifier that takes the form of a Universally Unique ID. The operation's *mode* has one of the values *In*, *Out*, *In/Out*, and *Out/In*. Depending on the mode, each operation has input parameters, output parameters, or both. A parameter has a name and data type associated with it. XML Schema data types can be adopted as a canonical type system for input and output parameters.

Semantic properties: the semantic of *Operations* is crucial to discovering Grid services. Semantic properties defined for operations include *Pre-condition*, *Post-condition*, and other domain specific properties.

Operational properties: we propose to provide *Operations* with *Scenarios* as operational properties that can be used to validate business model and service model. *Scenarios* of low-level component specification are designed based on *Scenarios* of high-level component specification [18]. Due to the limited space, we don't discuss them in detail.

Registered service: the registered service is an implemented web service. Let us distinguish between abstract operation and concrete operation. An abstract operation only specifies the requirements without referring to any specific service implementation. A concrete operation specifies the requirements and web location of the service.

In component specification, *Behavior* describes another kind of semantic information of *Operations* by using formalisms like finite state transition system. Generally speaking, not all the operation sequences are permitted. *Behavior* is used to determine valid order of *Operations*.

Resources record resources that can be accessed by the specified component.

Choreography carries information about the expected participant partners, operations, and the expected collaborative process between participants.

Definition 3.5 (Component description) A component description is a tuple $D=(\theta, \Phi, E)$, where:
• θ is a set containing signatures of component description.
• Φ is a set of functional goal (operations) and constrains.
• E is the context of Φ, including *Global-goal*, *Choreography*, *Constituent Partners*, and so on.
Component description is used to define component specification independent of specific description logic.

Definition 3.6 (Scenario) Given a component description $D=(\theta, \Phi, E)$, a scenario for a component operation is a pair (M, V), where:
• M is a transition system structure $(W, w_o, \rightarrow, \Gamma)$, Γ is a set of activities of the given operation.
• V is a valuation function: $V: F \rightarrow W \rightarrow S$, F is formulas over θ (e.g., pre-condition and post-condition), S is the sort of a given formula f. $V(f)(w)$ returns the value of f at state w.
Scenario can be used to test the virtual organizations.

Definition 3.7 (Component specification) A component specification is a pair $C=(D, B)$, $D=(\theta, \Phi, E)$, B is a set of scenarios, and $B \models \Phi$.

$\models$ is defined as following: Given a operation $\varphi:<a(p,o)>\psi$, where p is input, o is output, φ and ψ are precondition and post-condition of $a(p,o)$ respectively, it is said to be satisfied by a scenario $b=(M, V)$, $M=(W, w_o, \rightarrow, \Gamma)$, written as $b \models \varphi:<a(p,o)>\psi$, iff there exists path: $w_0 w_1 ... w_n$, φ holds at w_0 ($V(\varphi)(w_0)$ is true), when $a(p,o)$ is executed, the state arrives at w_n, $<w_i, w_j> \in \rightarrow$, i, $j \leq n$, and ψ holds at w_n ($V(\psi)(w_n)$ is true).

By integrating scenarios into component specification, the operational requirement of the component composition is met. The behavior and properties of the composed component can be checked [17].

Component specification is used to select cooperation partner or Grid service by semantic matching.

The architecture based modeling approach results in three kinds of relationships among components: γ-relationships, β-relationships, and λ-relationship. In order to validate virtual organizations and to support discovery and composition of Grid services by means of automated tools, the mentioned relationships and relationship compositions should have rigorous semantic.

Definition 3.8 (γ-relationship: Responsibility-Assignment) Let

$C_1=(D_1, B_1)$ and $C_2=(D_2, B_2)$ be component specifications, where $D_1=(\theta_1, \Phi_1, E_1)$, $D_2=(\theta_2, \Phi_2, E_2)$, B_1 and B_2 are scenario sets of C_1 and C_2 respectively. γ: $C_1 \rightarrow C_2$ means that Φ_1 is the global-goal of Φ_2, and $B_1 \models \Phi_1 \Rightarrow B_2 \models \Phi_2$, $B_2 \not\models \Phi_2 \Rightarrow B_1 \not\models \Phi_1$.
γ-relationship describes the decomposition of high-level goal, and answers the question "why a component exists?".

Definition 3.9 (β-Relationship: Take-Part-In) Let $C_1=(D_1, B_1)$ and $C_2=(D_2, B_2)$ be component specifications, where $D_1=(\theta_1, \Phi_1, E_1)$, $D_2=(\theta_2, \Phi_2, E_2)$, B_1 and B_2 are scenario sets of C_1 and C_2 respectively. β: $C_1 \rightarrow C_2$ means that:
• the constituent partners of C_2 contains C_1;
• Φ_1 is the sub-goal of Φ_2, and $B_2 \models \Phi_2 \Rightarrow B_1 \models \Phi_1$, $B_1 \not\models \Phi_1 \Rightarrow B_2 \not\models \Phi_2$.
β-Relationship can be used to trace how a component cooperates with others.

Definition 3.10 (λ-relationship: Achieved-By) Let $C_0=(D_0, B_0)$ be an abstract component specification (only contain requirements) and $C=(D, B)$ be a composite component specification, where $D_0=(\theta_0, \Phi_0, E_0)$, $D=(\theta, \Phi, E)$, B_0 and B are scenarios of C_0 and C respectively. λ: $C_0 \rightarrow C$ means that:
• $\Phi_0=\Phi$;
• $B \models \Phi \Rightarrow B_0 \models \Phi_0$.
λ-Relationship helps stakeholders to trace how the global goal is achieved.

Definition 3.11 (Semantic based virtual organization model) A semantic based virtual organization model is a tuple $V_M=(B_M, \{\lambda_i: R_i \rightarrow G_i | i \in N\}, S_M)$, where B_M is business model, S_M is service model, R_i is a role of B_M, G_i is a service component of S_M.
When a partner want to join virtual organization the semantic based model is used to check whether the partner conforms to the role specification and the related role relationships.

Theorem 3.1 Let $R_0 \rightarrow_\lambda R\{R_i | i \in N\}$ be a business pattern. If there exist $\{\lambda_i: R_i \rightarrow G_i | i \in N\}$, where G_i is service component, then there exists $R_0 \rightarrow_{\lambda'} G\{G_i | i \in N\}$, where G is composite component of $\{G_i | i \in N\}$.

According to Definition 3.8, Definition 3.9, Definition 3.10, Theorem 3.1 is hold obviously. The formal component relationships can be used to understand and to verify the constructed component model. We have discussed the semantic of relationship compositions in [19]. They are omitted due to the limited space.

Theorem 3.1 means that: 1) Given a well-defined business model (the role relationships have been verified), if the business goals of the roles can be satisfied by discovered Grid services then the virtual organization will operate correctly; 2) When Grid services changed, if the related component relationships remain the same then the virtual organization will run correctly.

4. CASE STUDY

The example used in this section is a simplified version of virtual newsroom model for newspaper publication. Currently, mobile office and home office are the main trends. The newsroom has been becoming virtual organization supported by Web/Grid services. For example, the editing departments are virtual teams in which the partners collaborate with each other by means of Web to edit and to publish newspapers, and the digital news library and press resources (i.e., RIP machines, Printers, and so on) are shared as common resources.

Three organization patterns of the business model are given as following (in order to depict role function intuitively, some roles are named after business operations) :

• *Newspaper Publishing*$\rightarrow_{\lambda 1}$*Newsroom*{*Page Editing*, *News Collecting*, *Paper Subscribing*, *Newspaper Pressing* }
• *Page Editing*$\rightarrow_{\lambda 11}$*Dept. of Page Editing*{*Page Proofing*, *Page Reviewing*, *Page Making* }
• *Newspaper Pressing*$\rightarrow_{\lambda 41}$*Pressing Center*{*Job Scheduling*, *Business Managing* }

Newspaper Publishing contains the business goal of *Newsroom* that is decomposed and assigned to *Page Editing*, *News Collecting*, *Paper Subscribing*, and *Newspaper Pressing*.
Newsroom describes the execution process of the business operations *Page Editing*, *News Collecting*, *Paper Subscribing*, and *Newspaper Pressing*. *Dept. of Page Editing* describes the execution process of the business operations *Page Proofing*, *Page Reviewing*, and *Page Making*. *Pressing Center* describes the execution process of the business operations *Job Scheduling* and *Business Managing*.

The organization patterns mentioned above specify three virtual organizations of different levels of granularity: *Newsroom*, *Dept. of Page Editing*, and *Pressing Center*. The organization patterns describe how to compose simple virtual departments into a complex virtual newsroom, and can be used as a foundation for virtual newsroom creation, evolution, and management.

Three service composition patterns of the service model are given as following:
• *Page Making*$\rightarrow_{\lambda 131}$ *Editor Service*{*News Retrieving*, *Page Typesetting*}
• *Page Reviewing*$\rightarrow_{\lambda 121}$ *Director Service*{*Page Checking*, *Reader Analyzing*}
• *Job Scheduling*$\rightarrow_{\lambda 411}$ *Job Controller Service*{*Job Assigning*, *Business Managing*}

News Retrieving, *Reader Analyzing*, and *Job Assigning* are Grid services that access Grid Resources *News Base*, *Reader Base*, and *RIP Network* respectively. *Editor Service*, *Director Service*, and *Job Controller Service* are service composite components.
Editor Service achieves business goal by means of two services: *News Retrieving* and *Page Typesetting*. *Director Service* also includes two services: *Page Checking* and *Reader Analyzing*.
In patterns given above, there exist three λ-relationships: λ_{131}: *Page Making*→*Editor Service*, λ_{121}: *Page Reviewing*→*Director Service*, and λ_{411}: *Job Scheduling*→*Job Controller Service*. *Page Making*, *Page Reviewing, and Job Scheduling* belong to the business model. *Editor Service*, *Director Service*, and *Job Controller Service* belong to the service model.

Due to the limited space, we don't give the component specifications.

By semantically defined component relationships, developers can verify the constructed patterns to find inconsistencies, can maintain complex relationships between component specifications, and can reveal hidden relationships. The semantic based virtual organization model can support organization evolution effectively. Traceability between organization goal and services can provide important insight

into virtual organization construction. When business goal are changed, the scope affected is determined by relationships of the components.

Development practices show that pattern is not only the right means to organize services and to construct business model but also the right means to record development expertise.

5. CONCLUSIONS

This paper applies architecture based modeling approach to construct semantic based virtual organization model. Compared with current researches, the main features of our approach are following: business model is constructed explicitly and semantically, it supports semantic match between business goal and Grid service; patterns are used to describe business component composition and service component composition; it supports virtual organization integration at varying levels of granularity; components and relationships are the main ingredients of the virtual organization model, recursive composition becomes an implicit and natural means for building complex virtual organizations; the component relationships have rigorous semantic, so that the hierarchical virtual organizations can be verified at configuration stage; patterns map business goals into services, the virtual organization maintainer profits from the traceability because he/she can understand why a virtual organization was built the way it was, and can better assess the impact of requirements or design modifications.

REFERENCES

[1] York Sure, Carole Goble, and Carl Kesselman, "Semantic Grid – Convergence of Technologies," http: // www. aifb. uni-karlsruhe. de /WBS/ysu/ publications/ semanticgrid-dag stuhl-seminar05271. pdf.

[2] David De Roure, Nicholas R. Jennings, And Nigel R. Shadbolt, "The Semantic Grid: Past, Present, and Future," in *Proceedings of The IEEE*, Vol. 93, No. 3, Mar 2005, pp.669~681.

[3] Luis M. Camarinha-Matos, "Virtual Organizations in Manufacturing: Trends and challenges," *FAIM'02*, Jul 2002, Dresden, Germany, pp.1~18.

[4] Wolfgang Emmerich, Ben Butchart, Liang Chen, Bruno Wassermann, Sarah L. Price, "Grid Service Orchestration using the Business Process Execution Language (BPEL)," *Research Note RN 05/07*, Dept. of Computer Science, University College London.

[5] Daniel J. Mandell, Sheila A. McIlraith, "A bottom-up approach to automating web service discovery, customization, and semantic translation," http:// www .daml .org/ services/ pubs/ www2003 sam-djm- workshop.pdf.

[6] Ye Zhang and William Song, "Semantic Description and Matching of Grid Services Capabilities," http:// www. allhands. org. uk /2004/proceedings/ papers/205. pdf.

[7] R. Bashroush, R. Perrott, "Using a Software Product Line Approach in Designing Grid Services," http:// www .allhands. org. uk/ 2005/ proceedings/ papers/499. pdf.

[8] Martin Hepp, Frank Leymann, Chris Bussler, et al, "Semantic Business Process Management: Using Semantic Web Services for Business Process Management". http:// dip. semanticweb. Org / documents/ Hepp-et-al-Semantic-Business-Process-Management-Using-Semantic-Web-Services-for-Business-pro.pdf.

[9] Yujian Fu, Zhijiang Dong, Xudong He, "Formalizing and Validating UML Architecture Description of Web Systems". http:// www. lcc.uma.es/~av/mdwe2006/camera_ready_papers/TransformationMDWE06-Fu.pdf.

[10] Matti Husu, "Software Factories," http:// www. cs. helsinki.fi/u/ thruokol/opetus/ 2006/ sose/ papers/husu_ software factories.pdf.

[11] Randy Howard and Larry Kerschberg, "A Framework for Dynamic Semantic Web Services Management". http:// eceb.gmu.edu/ pubs/IJCIS_Howard_Kerschberg. pdf.

[12] Shalil Majithia, David W.Walker, W.A.Gray, "Automated Composition of Semantic Grid Services," http:// www . wesc. ac. uk /resources/publications/pdf/ AHM04/148.pdf.

[13] Aniruddha Gokhale and Balachandran Natarajan, "Composing and Deploying Grid Middleware Web Services using Model Driven Architecture". http:// www .dre. vanderbilt.edu/~gokhale/WWW/ papers/ doa02-grid.pdf.

[14] Laura Bocchi, Paolo Ciancarini, Rocco Moretti, Valentina Presutti, Davide Rossi, "An OWLS Based Approach to Express Grid Services Coordination". http:// www .cs. unibo.it/ ~bocchi/papers/sac_ready.pdf.

[15] Maria Cecília Gomes, José C. Cunha, Omer F. Rana, "A Pattern-based Software Engineering Tool for Grid Environments," http:// asc. di. fct.unl.pt/ ~jcc/pub/nato- gomes-cunha-rana.pdf.

[16] Mike Uschold, Martin King, Stuart Moralee and Yannis Zorgios, "The Enterprise Ontology," http:// www. eee-con.de / german / information/ 98-ker-ent-ontology. pdf.

[17] Carlos Granell, Michael Gould, Roy Grønmo, David Skogan, "Improving reuse of web service compositions," http:// www . geoinfo . uji.es / pubs/ecweb05.

[18] CHU Wang, QIAN Depei, "Support Test Design Reuse by Architecture based Modeling," *J. Huazhong University of Science & Technology (Nature Science Edition)*, Vol.33, Dec 2005, pp.184~186.

[19] CHU Wang, QIAN Depei, "Formal Semantic of Architecture-Centric Component Model," *Journal of Softwar*e, Vol.17, No.6, Jun 2006, pp.1287~1297.

Cross-Layer Optimization Model for UWB Sensor Network

Yefang Gao [1,2] , Layuan Li [3] , Lin Ouyang [1]
[1]School of Information Engineering, WHUT, Wuhan, 430063, China
[2] Unit 94748, Network Center, Nanjing, 210008, China
[3] School of Computer Science & Technology, WHUT, Wuhan, 430063, China
Email: yefanggao@whut.edu.cn

ABSTRACT

Cross-layer design is a promising approach to improve the performance of wireless sensor networks. This paper studies an UWB-based wireless sensor networks and builds a cross-layer optimization model with joint consideration of MAC layer scheduling, PHY layer power control and network layer routing. The model takes advantage of significant benefits of UWB technology, such as huge bandwidth, extremely low power spectral density and large processing gain in the presence of interference and attempts to achieve the maximal data rate of whole network. Simulation results show that the optimal solution of cross-layer optimization model can increase the data rate of network obviously. It also demonstrates that it is feasible and effective to address issues of cross-layer problem with optimization model.

Keywords: UWB, Wireless Sensor Networks, Cross-Layer Design, Optimization Model

1. INTRODUCTION

Ultra Wide Band (UWB) radio is a kind of impulse radio technique based on the modulation of short, nanosecond, low power pulses that is widely used in radar applications. In recent years, however, UWB has also received increasing attention for its significant benefits to wireless communication systems including Ad Hoc networks and wireless sensor networks[1-5]. In this paper, we study an UWB-based sensor network for environmental surveillance application. For this application, once special event detection, e.g. Air Pollution Index (API) abnormal increase, all sensing data must be relayed to a central data collection point, which is called base-station. The large-scale nature of sensor network, both in terms of the amount of sensors and the distributing area of network, introduce some unique challenges [6-7]. Specifically, due to interference from nearby links, a change of power level on one link will have noticeable impact on capacity of all neighboring links. Thus the routing problem at the network layer is associated with issues of other layers such as MAC layer scheduling and PHY layer power control. Hence, the network level problem must be pursued via a cross-layer approach [8-11].

2. NETWORK MODEL

We consider a UWB-based senor network of N sensor nodes and *one* base-station. Suppose there are n nodes in network that have detected certain events and each of them generated sensing data. Then the fundamental issue for this network is the following: Is it possible to relay all these data to base station?

2.1 Definition

In this paper, we attempt to deal with the data traffic problem via an optimization modeling approach. At first, we give the following definitions for the *feasibility* of rate vector r form the point of view of optimization modeling.

DEFINITION 1. Rate vector $r(r_1,r_2...r_n)$ consists of n elements, r_i is the data rate of node $i \in N$, $r_i > 0$ indicates that node i is a source node which producing sensing data upon an event detection.

DEFINITION 2. Rate vector r is *feasible* if and only if there exits one or more feasible solution such that r can be relayed to base station.

It is clear that the feasibility of rate vector r is associated with several issues from different layers of protocol stack of wireless sensor networks: *MAC layer*, dealing with how to allocate link resources for access among the nodes; *PHY layer*, determining the transmission power level for each node in a given scheduled access to the channel; *Network Layer*, choosing a appropriate path from which data can be routed from source nodes to base-station [12]. Clearly, this is a cross-layer problem that associated with scheduling, power control and routing.

2.2 Scheduling

MAC Scheduling deals with how to allocate link resources for access among nodes in network. In this paper, we regard spectrum as the resource to be allocated, although this method can be also used to time-slot systems. Hence, the role of MAC layer is allocating spectrum resource between competing nodes. Suggested by the proposals of TI, Xtreme, Intel and Time Domain for IEEE 820.15.3a Task Group[13]-[16], we adopt the Multi-Band CDMA scheme in this paper. That is, we divide total available UWB spectrum into M sub-bands. For each node in network, it chooses one or more sub-bands to transmit or receive data in CDMA manner. According to the regulation of FCC (Federal Communication Commission) [17], the total available UWB spectrum W is 7.5GHz (from 3.1 GHz to 10.6 GHz), the minimum bandwidth of UWB is 500MHz. We divide W into M sub-bands. For a given number of total sub-bands M, MAC scheduling deals with following questions: (1) How to distribute the total spectrum W into M sub-bands? (2) In which sub-band a node should transmit or receive data? Denote $w^{(m)}$ as the bandwidth of sub-band m. we have

$$\sum_{m=1}^{M} w^{(m)} = W \tag{1}$$

$$w_{min} \le w^{(m)} \le w_{max}, \quad 1 \le m \le M \tag{2}$$

$$\begin{aligned} w_{min} &= 500 \\ w_{max} &= 7500 - (M-1)w_{min} \end{aligned} \tag{3}$$

2.3 Power Control

Denote p_{ij}^m as the power spent by node *i* in sub-band *m* for sending data to node *j*, for $\forall i \in N$, its power spectral density must satisfy the following limit [18]

$$\frac{g_{nom}\sum_{j\in N_i} p_{ij}^m}{w^{(m)}} \le p_{max} \tag{4}$$

where p_{max} is the upper limit of power spectral density(PSD) for UWB devices, g_{nom} is the gain at nominal distance, and N_i is the set of nodes to which node *i* can send data directly in one hop. From Eq.(4), we have

$$\sum_{j\in N_i} p_{ij}^m \le \frac{w^{(m)} p_{max}}{g_{nom}} \tag{5}$$

Eq.(5) defines the upper limit of power spent by node *i* in sub-band *m*. The maximum data rate of a noisy channel is given by Shannon Equation [12]

$$\begin{aligned} C &= Blog_2(1+\frac{S}{N}) \\ &= Blog_2(1+\frac{S}{N_1+N_2}) \end{aligned} \tag{6}$$

in Eq.(6), *B* is channel bandwidth, *S/N* is Signal-to-Noise Ratio(SNR), N_1 is the power of ambient Gaussian white noise, N_2 is the interference power produced by other nodes in network. Denote I_i as the set of nodes which can make interference at node *i*. The link capacity from node *i* to node *j* in sub-band *m* is

$$\begin{aligned} c_{ij}^m &= w^{(m)} log_2(1+\frac{S}{N_1+N_2}) \\ &= w^{(m)} log_2(1+\frac{g_{ij}p_{ij}^m}{\eta w^{(m)} + \sum_{k\in I_j, l\in N_k}^{k,l\ne i,j} g_{kl}p_{kl}^m}) \end{aligned} \tag{7}$$

where η is the power spectral density of ambient Gaussian white noise, $g_{ij}=d_{ij}^{-2}$ is the propagation gain from node *i* to node *j*, d_{ij} is the distance between node *i* and node *j*, and $k,l\ne i,j$ means $k=i$ and $l=j$ can not happen at the same time.

2.4 Routing

To take full advantages of multi-band communication, we divide the data flow from source node into several sub-flows and permit them take different paths to next nodes. Denote f_{ij} as actual data rate from node *i* to node *j*, then we have

$$f_{ij} \le \sum_{m=1}^{M} c_{ij}^m \tag{8}$$

Eq.(8) indicates that the link capacity is the upper bound of actual data rate. Furthermore, for $\forall i \in N$, it still follow the flow balance constrain described in Eq.(9).

$$\sum_{j\in N_i} f_{ij} - \sum_{j\in S_i} f_{ji} - r_i = 0 \tag{9}$$

where S_i is the set of nodes that can send date to node *i*. Note, if node *i* is not a source node then $r_i=0$.

3. CROSS-LAYER OPTIMIZATION MODEL

3.1 Link Capacity of Sub-Band

Due to the inherently low SNR nature of UWB technology [17], we have

$$\frac{S}{N} = \frac{g_{ij}\cdot p_{ij}^m}{\eta w^{(m)} + \sum_{k\in I_j, l\in N_k}^{k,l\ne i,j} g_{kj}p_{kl}^m} << 1 \tag{10}$$

Introduce the linearity approximation of the log function, i.e., $\ln(1+x)\approx x (x<<1)$, we have

$$\begin{aligned} c_{ij}^m &= w^{(m)} log_2(1+\frac{g_{ij}p_{ij}^m}{\eta w^{(m)} + \sum_{k\in I_j, l\in N_k}^{k,l\ne i,j} g_{kj}p_{kl}^m}) \\ &= w^{(m)} \frac{\ln(1+\frac{g_{ij}p_{ij}^m}{\eta w^{(m)} + \sum_{k\in I_j, l\in N_k}^{k,l\ne i,j} g_{kj}p_{kl}^m})}{\ln 2} \\ &\approx \frac{w^{(m)}}{\ln 2}\cdot\frac{g_{ij}p_{ij}^m}{\eta w^{(m)} + \sum_{k\in I_j, l\in N_k}^{k,l\ne i,j} g_{kj}p_{kl}^m} \end{aligned} \tag{11}$$

Eq.(11) is equivalent to

$$\begin{aligned} c_{ij}^m &= \frac{w^{(m)}}{\ln 2}\cdot\frac{g_{ij}p_{ij}^m}{\eta w^{(m)} + \sum_{k\in I_j, l\in N_k}^{k,l\ne i,j} g_{kj}p_{kl}^m} \\ &= \frac{w^{(m)}}{\ln 2}\cdot\frac{g_{ij}p_{ij}^m}{\eta w^{(m)} + \sum_{\substack{k\in I_j \\ l\in N_k}} g_{kj}p_{kl}^m - g_{ij}p_{ij}^m} \end{aligned} \tag{12}$$

Eq.(12) can be used to calculate the link capacity of node *i* to node *j* in sub-band *m*. To write Eq.(12) in a more compact form, we introduce symbol *q*

$$q = \frac{p}{\eta} \tag{13}$$

Eq.(5) and Eq.(12) can be rewritten as follow

$$\sum_{j\in N_i} q_{ij}^m \le \frac{w^{(m)} q_{max}}{g_{nom}} \tag{14}$$

$$c_{ij}^m = \frac{w^{(m)}}{\ln 2}\cdot\frac{g_{ij}q_{ij}^m}{w^{(m)} + \sum_{\substack{k\in I_j \\ l\in N_k}} g_{kj}q_{kl}^m - g_{ij}q_{ij}^m} \tag{15}$$

3.2 Cross-Layer Optimization Model

In [8], Radunovic and Le Boudec advocate the use of $\sum_l^L lnr_l$ as a utility metric in the network optimization problem. The reason for this choice is that such log-based utility function can make a good compromise between fairness and efficiency. In this paper, however, our purpose is to achieve the maximum data rate of network. So we introduce optimal factor *K* and use *MAX K* as objective function of our optimization model. In this way, the cross-layer design problem convert to a maximization problem for the maximal rate vector $K_{max}r$ under the optimization space of scheduling, power control, and routing. If the optimization model yields $K_{max}\ge 1$, it means there exists a solution which ensure rate vector $K_{max}r$ (bigger than *r*) be relayed to base-station successfully, then we claim the rate vector *r* is feasible; otherwise (i.e., $K_{max}<1$), it means the current solution can only ensure a rate vector that less than *r* be relayed to base-station, we say that the current rate vector *r* is infeasible(see DEFINITION 1). Using Eq.(1)~(15), we formulate the cross-layer optimization model as follows.

Objective Function

$$\max = K$$

Schedule Constraints

$$\sum_{m=1}^{M} w^{(m)} = 7500$$

$$w_{min} \le w^{(m)} \le w_{max}, \quad 1 \le m \le M$$

Power Control Constraints

$$\sum_{j\in N_i} q_{ij}^m - \frac{Wp_{max}}{g_{nom}\eta} w^{(m)} \le 0 \quad 1 \le i \le N, 1 \le m \le M$$

$$c_{ij}^{m} = \frac{w^{(m)}}{\ln 2} \cdot \frac{g_{ij} \cdot q_{ij}^{m}}{w^{(m)}\eta + \sum_{k \in I_j, l \in N_k} g_{kj} q_{kl}^{m} - g_{ij} q_{ij}^{m}}$$

$$1 \le i \le N, j \in N_i, 1 \le m \le M$$

Route Constraints

$$f_{ij} \le \sum_{m=1}^{M} c_{ij}^{m} \quad 1 \le i \le N,\ j \in N_i$$

$$\sum_{j \in N_i} f_{ij} - \sum_{j \in S_i} f_{ji} - K r_i = 0 \quad 1 \le i \le N$$

4. SIMULATION

4.1 Simulation Setting

In this section, we present the simulation results of cross-layer optimization model through a small network of 25 sensor nodes (mark as triangles) and 1 base-station (mark as solid circle) (see Fig.1). There are 2 source nodes (marked as solid stars) in network, and the data rate of them are $r_5=4$ and $r_{25}=5$ with units Mb/s. The total UWB spectrum is 7.5GHz and the minimum bandwidth of each sub-band is 500MHz. The communication radius of sensor node in network is 10 meters [17]. The nominal gain g_{nom} is 0.02, and power spectral density limit p_{max} assumed to be 1% of η [18].

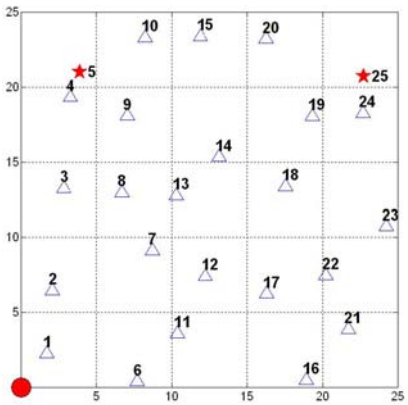


Fig.1. Network topology for 25-nodes network.

4.2 Results and Analysis

In simulation, we resolve optimization model with different M, and get the maximum achievable K_{max} as a function of M, see Fig.2.

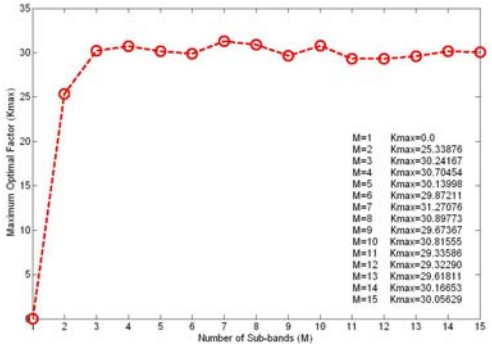


Fig.2. The K_{max} as a function of M for 25-nodes network.

In Fig.2, when M is 1, namely, there is only one sub-band in network and it occupies total available UWB spectrum W, K_{max} is 0(r is infeasible). The reason rate vector $r(r_5,r_{25})$ can not be relayed to base-station is that nodes can not transmit and receive data in the same sub-band. Note, both *node 5* and *node 25* are not one-hop neighbors of base-station(see Fig.1), and this implies that data rate form them must be relayed by other nodes around them. For any node which can receive data from *node 5* or *node 25*, there is only one sub-band for this node to use. So if it receives data form source node, it can not transmit data through the same sub-band again. On the other hand, when there are two or more sub-bands in network($M \ge 2$), the K_{max}s are all great than 1(from 25.33876 to 31.27076). In these instances, the rate vector $r(r_5,r_{25})$ is feasible and can be relayed to base-station successfully.

Also, in Fig.2, it is clear that there is a obvious increase in K_{max} as M is relative small (M=2~4). But when M>4, the K_{max} becomes regular. The curve in Fig.2 is different to some extent from Shiyi's work in [19]. In [19], K_{max} is a progressive increase function of M, which is quite different from our results. Through comprehensive discuss with Shiyi, we come to the conclusion that the different termination criterion of solution producer and the different calculate method for propagation gain are the primary causes which lead to the difference between results of his and our research. Firstly, in[19], for the purpose of reducing solution time, the solution producer stops as soon as it get any feasible solution with $K_{max} \ge 1$, thus the K_{max} is quite likely to be a local optimal solution. In our paper, however, we apply a so-called multi-start solution procedure. Namely, we adopt a strategy that restarts the procedure several times from different initial points within optimization space (e.g.,100 points) and select the best local solution as the final optimal solution of model. Multi-start strategy has proven successful for models with multi-convex nature[20]-[21], so the K_{max}s of our work are quasi-global optimal solutions and thus are closer to the fact than that of [19]. Secondly, in order to prevent nodes from transmitting and receiving data within the same sub-band, both Shiyi and we introduce a notion called self-interference parameter g_{jj} (see Eq.12). In [19], propagation gain is given by $g_{ij}=min(d_{ij}^{-2},1)$ which lead to g_{jj} equal to 1 during solution procedure. But by several experiments, we found $g_{jj}=1$ can not achieve above purpose. In other words, when node j is transmitting data to any node l, the link capacity on node i to j is not *zero* and this will result in any node i could send data to nod j in sub-band m even if j is transmitting data to node l in the same sub-band. That is to say, some data rates received by base-station in [19] are *inexistent* in fact. And we believe this is the reason why K_{max} is a progressive increase function of M in [19]. In our works, however, we set g_{jj} as a very big real number, e.g. g_{jj}=10000. In this way, when node j is transmitting data to any node l, the link capacity on node i to j (c_{ij}^{m}) can effectively shut down to 0 (for the reason of calculate error, c_{ij}^{m} is not 0 actually, but it is of the order of magnitude of 10^{-5}~10^{-7}).

Fig.2 can be explained with Shannon Equation (Eq.6) as follow: as M grows bigger, there are more sub-bands for nodes to choose when they have data to send, that is, the more opportunity for nodes to avoid interference with other nodes within the same sub-band. So, the N_2 in Eg.(6) decreases and this results in the increase of signal-to-noise ratio (S/N), as a result, the link capacity C increases; but on the other hand, as M grows bigger, the bandwidth of sub-band m $w^{(m)}$ becomes smaller, namely, the increase of M means the decrease of B in Eg.(6), and this will lead to the decrease of C at last. In a word, we can draw a conclusion from Fig.2: when M is small, the influence of S/N upon link capacity C is much bigger than that of M; but as M becomes bigger, for example, M>4, the

influence of M upon C increase and counteract the influence of S/N upon C. Furthermore, the curve in Fig.2 also suggests that to resolve the model in shorter time with enough numerical precision, we could just choose a small value (e.g., M=4) for the number of sub-bands instead of the bigger one (e.g., M=15).

Denote $K_{max}\sum r_i$ as maximum achievable data rate of network. Table 1 and Table 2 shows $K_{max}\sum r_i$ and actual data rate between nodes for M=4 respectively($w^{(1)}$= 1714.377, $w^{(2)}$= 1714.377, $w^{(3)}$= 1731.909, $w^{(4)}$= 2339.337). These results satisfies scheduling, power control and routing constraints described in optimization model, and demonstrates the feasibility and efficacy of optimization modeling approach to cross-layer design problem.

5. CONCLUSIONS

In this paper, we studied issues of data traffic for UWB-based sensor networks. We built a cross-layer optimization model with joint consideration of MAC layer scheduling, PHY layer power control and network layer routing. Simulation results show the optimal solution of proposed model can increase the data rate of network obviously and demonstrate it is feasible and effective to deal the cross-layer problem with optimization model. However, the optimization model described in this paper is a NLP (Non-Linear Programming) model, which remains NP-Hard problem in general [20-21]. It can only handle small-scale networks at present. For large scale network, it is quite likely beyond the capability of an ordinary computer. Therefore, developing a more suitable model for large-scale network will be the emphasis of our future research.

REFERENCES

[1] M.Z.Win, R.A.Scholtz, "Ultra-wide bandwidth time-hopping spread-spectrum for wireless multiple-access communications," *IEEE Trans. Commun.*, vol. 48, 2000, pp. 679~689.

[2] M.Z.Win, R.A.Scholtz, and M.A.Barnes, "Ultra-wide bandwidth signal propagation for indoor wireless communications," in Proc. *ICC Montreal, Toward Knowledge Millennium*, vol.1,1997,IEEE Int. Conf. Communications, pp.56~60.

[3] M.Z.Win, R.A.Scholtz, "Impulse radio: How it works," *IEEE Commun. Lett*., vol. 2, pp. 36–38, 1998.

[4] F.Ramirez-Mireles, M.Z.Win, and R.A.Scholtz, "Performance of ultra-wideband time-shift-modulated signals in the indoor wireless impulse radio channel," in *31st Asilomar Conf. Signals Systems Computers*, vol.1, 1997, pp. 192~196.

[5] F.Ramirez-Mireles, R.A.Scholtz, "Multiple-access performance limits with time hopping and pulse position modulation," *MILCOM*, 1998, vol.2, pp. 529~533.

[6] Lan F.Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, 2002,40(8), pp.102~114.

[7] David Culler, Deborab Estrin, Mani Srivastava. "Overview of Sensor Networks," *IEEE Computer*, Vol.37, Issue.8, 2004, pp.41~49

[8] B. Radunovic and J.-Y. Le Boudec. "Optimal power control, scheduling, and routing in UWB networks," *IEEE J. Selected Areas in Commun.*, vol.22, no.7, 2004, pp.1252~1270.

[9] Madan,R., Shuguang Cui et al, "Cross-Layer Design for Lifetime Maximization in Interference-Limited Wireless Sensor Networks," In *Proc. INFOCOM 2005*,Vol. 3, pp.1964~1975

[10] Kozat, U.C., Koutsopoulos, I. et al, "A Framework for Cross-layer Design of Energy-efficient Communication with QoS Provisioning in Multi-hop Wireless Networks," In *Proc. INFOCOM 2004*. Vol.2, pp. 1446~1456

[11] Pierre Baldi, Luca De Nardis et al, "Modeling and Optimization of UWB Communication Networks Through a Flexible Cost Function, " *IEEE J. on Selected Areas in Commun.*, Vol.20, No.9, 2002, pp.1733~1744

[12] Andrew S. Tanenbaum, *Computer Netwroks(3rd Edition)*, Prentice Hall, 2004, pp.77~479

[13] Batra A,et al, "TI Physical Layer Proposal for IEEE 802.15 Task Group 3a," *IEE*E 802.15-03/142r0, 2003.

[14] Robert R.. "Xtreme Spectrum CFP Document," *IEEE 802*.15-03 /154r1, 2003.

[15] Foerster J, et al, "Intel CFP Presentation for a UWB PHY," *IEEE 802*.15-03/109r1, 2003.

[16] Kelly J, "Time Domain's Proposal for UWB Multi-band Alternate Physical Layer for 802.15.3a," *IEEE 802*.15-03/142r2, 2003.

[17] "First Report and Order in the Matter of Revision of Part 15 of the Commission's Rule Regarding Ultra-Wideband Transmission System," ET Docket, Federal Communication Commission, FCC 02-48, 2002, pp.98~153

[18] A.Rajeswaran, G.Kim, R.Negi, "A scheduling framework for UWB &c ellular networks," in *Proc. First International Conference on Broadband Networks*, 2004, pp.386~395

[19] Yi Shi, Y.T.Hou et al, "Cross-Layer Optimization for Routing Data Traffic in UWB-based Sensor Networks," in *Proc. MobiCom'05*, 2005, pp.299~312.

[20] Giordano F.R., *Weir M.D et al, A First Course in Mathematical Model (3rd Edition)*, Californian: Brook/Cole, 2003.

[21] Winston W.L., *Introduction to Mathematical Programming (4rd Edition)*, Californian: Brook/Cole, 2003.

Yefang Gao was born in 1970. He received M.A's. degree in CAD from Nanjing University of Science and Technology, Jiangsu, China, 1999. Since 2004, he has been a Ph.D. degree candidate in School of Information Engineering, Wuhan University of Technology, Hubei, China. His current research interests include UWB communication and wireless sensor networks.

Layuan Li was born in 1946. He received ME degree in Communication and Electrical System from Huazhong University of Science and Technology ,China in 1982. He is currently a professor and Ph.D tutor of Computer Science. His research interests include computer networks, protocol engineering and image processing.

Lin Ouyang, was born in 1974. He is a Ph.D candidate in School of Information Engineering, Wuhan University of Technology, Hubei, China. His research interests are in distributed parallel processing, Artificial Intelligence and computer network.

Table 1. Maximum Achievable Data Rate of Network for M=4

M	K_{max}	$K_{max}\sum r_i$	M	K_{max}	$K_{max}\sum r_i$	M	K_{max}	$K_{max}\sum r_i$
1	0	0	6	29.87211	268.84899	11	29.33586	264.02274
2	25.33876	228.04884	7	31.27076	281.43684	12	29.32290	263.90610
3	30.24167	272.17503	8	30.89773	278.07957	13	29.61811	266.56299
4	30.70454	276.34086	9	29.67367	267.06303	14	30.16653	271.49877
5	30.13998	271.25982	10	30.81555	277.33995	15	30.05629	270.50611

Table 2. Actual data rate f_{ij} for M=4

node-node	f_{ij}	node-node	f_{ij}	node-node	f_{ij}	node-node	f_{ij}
1-0	249.0988	7-2	31.50501	17-11	37.19610	23-21	33.37935
2-1	134.5733	8-2	43.57650	17-12	43.91400	23-22	36.92747
3-2	59.49176	9-8	43.57650	18-12	35.02987	24-18	23.22242
4-3	59.49176	10-14	19.74990	18-22	11.28157	24-23	39.97001
5-4	59.49176	11-1	30.49871	19-14	20.78144	25-18	14.40208
5-9	43.57650	11-6	69.84775	19-18	8.686938	25-19	59.80519
5-10	19.74990	12-6	17.02137	19-23	30.33681	25-20	16.12300
6-0	27.24208	12-11	62.67207	20-14	16.10241	25-24	63.19243
6-1	59.62704	13-7	56.65435	21-17	32.90106		
7-1	24.39977	14-13	56.65435	22-17	48.20904		

Semantic Caching in Mediator System*

Nianbin Wang[1], Shengchun Deng[2], Daxin Liu[1], Zhiqiang Zhao[1]
[1] Department of computer Science and Technology, Harbin Engineering University
Harbin, 150001, P.R China
[2] Department of computer Science and Technology, Harbin Institute of Technology
Harbin, 150001, P.R China
Email: {Wangnianbin, Liudaxin, Zhaozhiqiang} @hrbeu.edu.cn, DengshengChun@hit.edu.cn, wnberp@yahoo.com.cn

ABSTRACT

HPDPM system is a mediator system using semantic caching technology to support large scale data manipulating. As an important method to improve system performance, semantic caching is often used in client's end. In the light of HPDPM application environment, this paper researched an approach which can be used in mediator system. Using semantic caching technology, it will greatly reduce interactions among mediator and servers, especially in semantic related environment. A semantic caching query processing method for improving system efficiency is given in detail, the replacement strategy and consistency management method are discussed also. Implementation and experiments of this study showed that this approach can improve system performance efficiently. At present, the mediator system which used semantic caching technology has been applied to a large engineering project which capacity of data is a little more than 1000 Gigabytes.

Keywords: Parallel Data Processing, Mediator System, Storage Management, Semantic Caching, System Implementation

1. INTRODUCTION

With the development of information integration, today more and more data sources exist in enterprise on various topics [1]. In this case, providing a method to manipulate data paralleling can greatly improve efficiency of data process. A significant trend in the commercial data processing field is the increasing support for parallel data processing [2].

HPDPM (High Performance Data Processing Mediator) was built to provide integrating views for clients. It can manipulate user's queries in parallel method. The aim of HPDPM is improving system performance, especially for large user groups and large scale information.

As more and more users use mediator system to query data, such as in large enterprise or web application, mediator system becomes a bottle neck itself. There is a great demand for latency tolerance technologies for fast answering user queries. Many latency tolerance techniques have been developed over the years. In generally, the two most important ones are caching and pre-fetching [3]. Caching technology can greatly reduce the interactions between clients and servers. But traditional caching schemes, such as page caching, intend to exploit the static spatial or temporal locality to improve system performance, therefore have inherent disadvantage [4].

Traditionally, semantic caching was used in client mainly. But HPDPM uses semantic caching in mediator system. The reason is lying in three factors: First, the application environment of HPDPM includes a great deal of users, placing semantic caching in client end will bring multiple workloads in system maintenance, because in this way, it needs to install software in client. Second, the configuration of client end in HPDPM system environment is not high, and its users often need to query large scale information, caching information in client can greatly reduce client's performance. The third, caching in mediator system can share information with more users, add hitting rate, and facility caching consistency maintenance.

The purpose of this study is therefore to research an approach using semantic caching in mediator system, which can improve the performance of mediator system efficiently. The rest of the paper is organized as follows: Section 2 discusses semantic caching application platform, the HPDPM system and its main functional architecture. Section 3 discusses semantic caching technology applying in mediator system. The semantic caching query processing, replacement strategies and consistency management methods are also discussed. Then, implementation and experiment of semantic caching in parallel data processing mediator system are presented in Section 4. Section 5 concludes the paper.

2. MEDIATOR SYSTEM

HPDPM System has been applied in Heilongjiang Local Taxing Bureau. It connects data and information from every city, district, and country with exclusive network, providing transparent services for its users.

Mediator system provides an integrated view for its users, it uses the data resources existing in whole grid providing an approach which can be used to answer user's query with facility and shortcut. The following context will describe the functional architecture of mediator system from the views of how to realize semantic caching.

2.1 System Functional Architecture

Based on Web browser and client's end, users can submit their queries. Mediator system finishes the whole job without user intervention. It decomposes query into sub-queries. If the query results are existed in semantic caching entirely, mediator will answer queries with the content of caches, or if the results are matched partially, mediator will count the difference, and send sub-query to related resource node, when the results return, mediator unites the whole results, and backing out.
HPDPM mainly includes there modules: building module, running module and information services module. The overall functional architecture is shown as fig.1.

2.2 Module Function

Building module is a system building environment provided by HPDPM system. Here administrator can build related information about resource nodes, communication mechanisms, connecting strategies and system configuration parameters, classify new node with system global views, and use ontology to eliminate semantic differences.

* Supported by National High-Tech Research and Development Plan of China (863-2003AA4Z3370).

The basic idea is based on domain shared ontology, making the same interpretation for data and commands, despite of syntactic or/and structural differences. Check of semantic affinity for interoperability, semantic mismatch analysis, using the method of semantic annotation of local conceptual schemata and services. Ontology-based reconciliation, with rules automatically derived from semantic annotation [5]. With this method, HPDPM can eliminate the semantic differences of data and information.

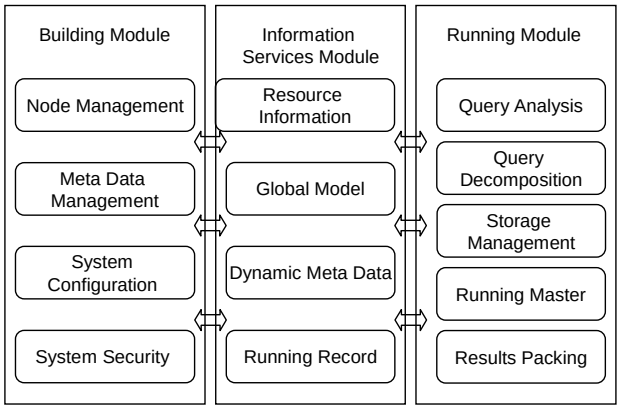


Fig.1. Functional Architecture of HPDPM system

The function of realizing user's query is finished by running module. When user submits query from client, the system monitors these query, and put them into agents, agent finishes every query and when query results come in, it returns results to user. As agent submits query to query analysis, query analysis first translates character string into system expression. Then determine if there exists caching result satisfied user query through storage management model.

When there is not semantic caching hitting, then query statement is put into query decomposer. Query decomposer analyses SQL statements, then decomposes the query into multi sub-queries according to meta data which stored in meta data dictionary.

Then executing controller acquires sub-queries, builds control mechanism, and submits every sub-query to remote data sources where the data exists. And when every data sources returns results, then controller trims the results and submits to agents. Using this method, mediator system finishes a user query. In this process, when query analysis finds that the user's query is in semantic caching entirely, we say the user's query is being hit totally.

In this case, mediator system needn't interact with servers, and it will put the results into results packing simply, and then return the answer to user directly.

Information services module mainly includes the mate data about the resources servers which acquired form building module, maintains a global views. Dynamic meta data block and running record block record the system running situations, facilitate running module making its query planning. Information Services module provides an information bases for the realization of semantic caching.

3. SEMANTIC CACHE IN MEDIATOR SYSTEM

This section focuses on research and design of semantic caching in mediator system. The idea of semantic caching is that the mediator system maintains both semantic descriptions and results of previous queries in the semantic cache. As a new query can be answered totally from the semantic cache, there is no need of communication happens between mediator system and data servers. One key advantages of the semantic caching is that the memory or disk space requirements and communication costs are reduced. Another advantage of semantic caching is its flexibility, which is very important for multi users and lager scale information situations. Page-cache is relatively inflexibility, because the content of the cache are dependent on the physical storage structure.

As a new query can only be partially answered, the original query is trimmed and the trimmed part is sent to the server and processed there. In this way, the amount of data transferred over the network can be substantially reduced.

3.1 Manipulating Query Based on Semantic Caching

According to the description of functional architecture, work principle of mediator system, this paper points out the aim of semantic caching is realization of fast responds, elimination of network loads. The efficiency of the semantic caching depends on how much the user's queries are related to each other, a lot of this kind of relations can be found in application system, in experiments of this paper, about 15% user queries are matched entirely, and 35-45% user queries are matched partially. In this situation, the results of earlier queries are contained in the results of later queries.

There are four possibilities [6], when semantic caching happens as fig.2. The white block represents semantic cache, black block represents user's query.

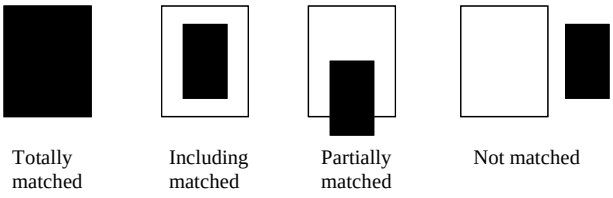


Fig.2. Semantic matched types

In case 1 "totally matched" and case 2 "including matched", semantic caching in mediator can answer user query without interaction with data server. In case 3 "partially matched" mediator system needs to count trim query, and sends query to related data server, then packs up the results. In case 4 "not matched", mediator system will send the whole user query to data server, then determine if mediator system need to cache query result and do related work.

Semantic cache is made up of a set of semantic blocks and a set of semantic items. In mediator system, query result is to be named a semantic block. Each semantic block is made up of a records set. Semantic items includes predicate which is in "where" cause of query statement.

When user's query belongs to case 3 or case 4, we say it needs semantic query manipulating. The match between the statement of user's query and the semantic items is the job worked by mediator to determine results differences. Then mediator will decompose the user query into two sub-queries. The results can not be acquired from semantic cache and the results can be acquired from semantic cache.

The first part is called the remote sub-query (*RQ*). The second

part is named the Local sub-query (*LQ*). Assumed each semantic block includes number of semantic items is N, and each item includes number of attributions is K. User query Q is made up of the conjunction of simple predicates, like $Q = q_1 \wedge q_2 \wedge \cdots \wedge q_k$. q_i corresponding semantic item's attribution S_i. The semantic caching manipulation algorithm is described as follow:

Caching Manipulation Algorithm

Input: query conditions $Q = q_1 \wedge q_2 \wedge \cdots \wedge q_k$ and semantic cache information { S_i };
Process: count Local sub-query (*LQ*) and remote sub-query (*RQ*).
Output: Results of *LQ* and *RQ*.

```
1:  for i ← 1 to n
2:    do C_{i,j} ←  S_{i,j}(j= 1,2,3,……k)
3:      for j ← 1 to k
4:        do LQ_{i,j} ← count intersection between q_j and c_{i,j}
5:              if  LQ_{i,j} = φ
6:                    then LQ_i ← F
7:                         goto 1
8:           LQ_i ← LQ_{i,1} ∧ LQ_{i,2} ∧ ⋯ ∧ LQ_{i,k}
9:              if  LQ_i = q
10:                then count(S_i) ← count(S_i) + 2
11:                     goto 15
12:                else count(S_i) ← count(S_i) + 1
13:              LQ ← LQ_1 ∨ LQ_2 ∨ ⋯ ∨ LQ_n
14:             if  LQ = q
15:               then RQ ← F
16:                 else RQ ← Q ∧ ¬LQ
17:                      end
```

The role of 'count' in line 10 and line 12 will be explained in following part.

3.2 Replacement Strategy

When the results of user's query are acquired from bottom servers, mediator system will put the results in semantic cache, if exists enough space in there. In multi-users environment, as semantic cache space is limited in fixed capacity, when new result is added to cache continuously, the cache space will be filled up. At this time, the mediator will consider replace some semantic blocks, in order to keep high hitting rates. In this paper, it is called cache replacement strategy.

The idea of cache replacement is to evaluate the probability of semantic blocks is visited by another queries effectively. In ideal situation, the blocks replaced by system should have lowest probability of being visited by user's queries.

In this study, the granularity of cache placement is a semantic block and semantic item. This paper believes that replacement based on visiting frequency on semantic item can effectively reflect user's attention to some items greatly.

Because the hitting rate of semantic caching is different from that of page caching, it includes 'totally matched', 'including matched' and 'partially matched' presented as figure 3. It's necessary to consider different cases. This paper uses the 'power value' of semantic items as a replacement value as formula (1).

$$\textbf{Power value} = \text{count}(S_i) + 1 / \text{size}(S_i) \quad (1)$$

Size (S_i) represents the number of the results set of semantic items, 1/Size (S_i) embodies the idea of replacement big results set as possible. Count (S_i) represents probability that the semantic items are matched by other query.
In algorithm 1, line 10, when query is matched totally, then count (S_i) = count (S_i) + 2, line 12, when query is matched including, then count (S_i) = count (S_i) + 1. In fact, the configuration of mediator remains the parameter as count (S_i) = count (S_i) + *N*. Administrator can adjust the parameter according to the application.

When cache does not have enough free space to hold the new data, the semantic blocks with the lowest power value will be discarded until there is enough space.

3.3 Consistency Strategy

When user wants to do some update (update, insert, delete) operation to information servers, mediator semantic caching will determine if the update will affect cache content. The consistency strategy of semantic caching is different from that of page caching. Because the granularity of semantic cache is the semantic item and block. An update to data in bottom server will probably affect multi semantic items. This paper applies object dependency graph to assist consistency maintenance. It includes two steps. First, according to attributes set and values of 'where' clause in query statement, system will build directed edges from result node to attribute nodes. Second, when update refers to attribute, locks the semantic items and prevents user query from visiting it. If update is success, then delete relation semantic blocks and items, else unlock the semantic items.

4. IMPLEMENTATION AND EXPERIMENTS

As before, a semantic cache consists of a set of semantic items which are defined by predicates and a set of semantic blocks which include result set. When a query comes, mediator will manipulate query according to algorithm 1. In this section, implementation and experiments are discussed in details.

4.1 System Implementation

The semantic caching in mediator includes a group of caching area and a semantic caching management mechanism described as fig.3.

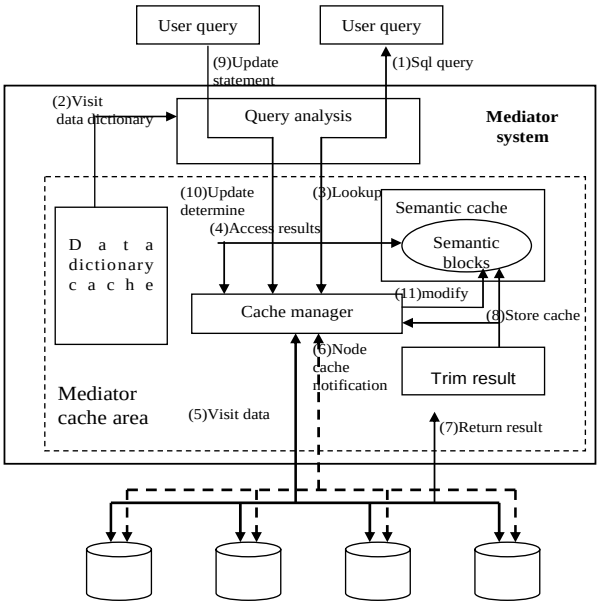


Fig.3. The work principle of semantic caching system

The caches include data dictionary cache, semantic cache and trimming cache. Data dictionary cache (DDC) is used to buffer database structure, user's information and data distributed information. In mediator system, every SQL statements submitted by user needs to visit DDC, in order to determine how to decompose SQL into multi sub-queries, and send those sub-queries to related node. Semantic cache (SC) is used to cache semantic items and semantic result. Items information includes statement cache and semantic items organized information. Statement cache mainly store SQL statements which results are in semantic cache. In this way, query analysis can rapidly match if a new user query can be found in semantic cache. Following this step, cache manager will query directly from semantic cache, and system will add the semantic items counter, modify its 'power values'. If a query can be found in semantic cache partially, system will decompose the statement into sub query, build local query (*LQ*) and remote query (*RQ*), and add the semantic items count, modify local query's 'power value'.

When semantic cache has not enough space to hold results set, system can determine how to realize replacement using 'power values'.

Trimming cache is a temp caching, when the result of queries return, it will first being put into trimming cache, and executing control will run result trim according to query analysis. For example, when user gives a SQL, like MAX salary, this SQL will probable be distributed to multi node, every node returns a MAX salary. In this case, we need to count real MAX salary in trimming cache by compare return value.

On of the most important Caching management problem is how to keep the data consistency. When user submits an update (update, insert, delete) statement, system must determine if it will affect the semantic caching consistency. And when the effect exists, caching manager will first lock the semantic segment and result in semantic caching, and until the update statement finished, and modify caching result, or simply give up the caching result which related to this modification.

4.2 System Experiments

To check the efficiency of semantic cache, this section examines the performance using 4 group query lists which are produced at random. Every group includes 200 queries, and the first 100 queries do not enter results data as a cache warm up data. Experiments include three aspects: semantic cache, traditional cache and no cache. The x-axis of the figure shows the different query group and different caching method. The y-axis of the figure is the average respond time of query.

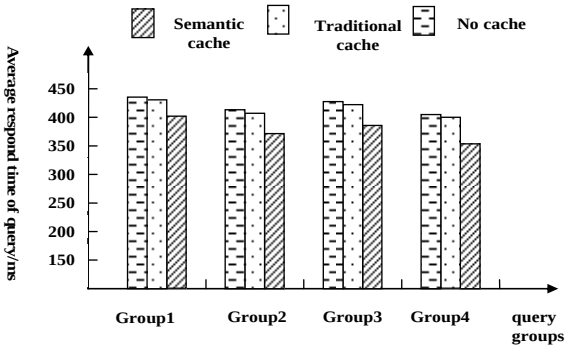


Fig.4. The average response time of query

Fig4 shows the average respond time of semantic cache method is better than that of traditional cache and no cache.
This study still researched the performance of semantic cache in field application area. Two important user's business activities named 'Declaring tax' and 'collecting query' is to be selected to check performance. The experiment results show as table 1. In table 1, the item of 'before' means not using semantic cache, the item of 'after' means using semantic cache. Being limited by condition, the data of 'before' is the average result of a whole year, the data of 'after' is the average result of three months.

As we can see from table 1, the query performance gained improvement distinctly. All declaring tax and collecting query refer to declaring people's related information, but the later business has stronger relationship with declaring information than the first business. Collecting query gained more improvement than that of declaring taxing. From this point, this study believes that the performance of semantic caching is extremely sensitive to the data semantic related. When a new query semantic related totally, query can gain maxed caching hitting, and when a new query semantic related partially, system need to spend extra cost to count the relation and acquire results.

Table 1 Application Testing

Business activity	Before (seconds)	After (seconds)
Declaring tax	0.45	0.36
Collecting query	1.42	0.85

5. CONCLUSIONS

Traditional semantic caching technique usually applied in client end. Based on the requirements of application, this paper presented a semantic caching scheme which is used in mediator system to improve system performance. A semantic caching method is given for improving system efficiency, include query manipulating algorithm, replacement strategy and consistency maintenance. Experiments showed that this scheme is in favor of improving mediator performance, especially in data semantic related application areas.
From the actually application environment, this study's query application exists about average 30% relation degree. But it lacks a determined query semantic relation dependency model which can be used to measure the relationship, so administrator has to determine related parameter with his experience, this situation adds the administrator's workload and error-prone. For future work, further investigation is needed to establish a model or method to solve the problem on how to measure the degree of semantic relation.

REFERENCES

[1] A.D.Jhingran,N.Mattos,"Information Integration: A Research agenda." *IBM System Journal*,Vol.41, No.4, 2002,pp.555-562.

[2] Anastassia Ailamaki, David J. DeWitt, Mark D. Hill. "DBMSs on A Modern Processor: Where dose Time Go,"*In Proceeding of the 25th VLDB Conference*, Edinburgh,Scotland,1999.

[3] Cheng-Zhong Xu,Tamer I. Ibrahim,"A keyword-based Semantic Pre-fetching Approach in internet News Services,"*IEEE Transactions on Knowledge and Data Engineering* ,Vol.16,No.5,2004,pp.601-611.

[4] K.Sattler,I.Geist,E. Schallehn,"Concept-based Querying

in Mediator Systems,"*Technical Report.* Department of Computer Science,University of Magdeburg,2003.

[5] Wang Nianbin,X.Xiaofei,"A Method to Build Ontology,"HPC-Asia2000,*the fourth International Conference on High Performance Computing in Asia-Pacific Regine*,Volume II,pp.672-674.

[6] P.Godfrey,J.Gryz,"Answering Query by Semantic Caches,"in *Database and Expert Systems Applications*. 10th Int. Conf.,DEXA'99,Italy,Proc,volume 1677of LNCS,pp.485-498,Springer,Aug,30-Sep,3,1999.

Nianbin Wang is a professor and vice director of high dependability computing technology research center in Harbin Engineering University. He graduated from Harbin Engineering University in 1990, and received the Ph.D. degree in Computer Science and technology from Harbin Institute of Technology in 2001. His research fields include Parallel Computing Technology, Large Scale Database System and Information integrating technology.

Shengchun Deng is an associate professor in Harbin Institute of Technology. He graduated from the Department of Computer Science and Technology of Harbin Institute of Technology in 1994, and received the Ph.D. degree in 2001. His research fields include large scale database system, enterprise information integration, and distrbuted computing.

A Multi-agent Architecture for Intelligent Distributed Surveillance Systems *

Xiaoling Xiao [1,2], Layuan Li [1]
[1] School of Computer Science and Technology, Wuhan University of Technology, Wuhan, Hubei, 430063, P. R. China
[2]Yangtze University, Jingzhou, Hubei, 434023, P. R. China
Email: xljrzx@163.com

ABSTRACT

The distributed surveillance systems include not only distributed array of cameras that offer wide area monitoring, but also a set of computer vision algorithms designed for scene analysis at multiple levels of abstraction. For building an intelligent surveillance system, the system requires the architecture for distributed computing environment to support real-time processing. This paper presents a multi-agent architecture for an intelligent distributed surveillance system. All processing modules in this system are encapsulated as agents. The proposed multi-agent architecture can be expressed by a multi-level concept. The surveillance system can be divided into 4 level tasks, which each level will be handled by one or several agents with different capabilities. Data management and transfer agent is a key module that supports real-time heterogeneous data stream sharing and exchanging among agents. Heterogeneous data and communication mechanism among agents are analyzed. The distributed surveillance system with the multi-agent architecture is currently applied as a test bed for the project that is based on meeting analysis and archive in intelligent meeting room in real-time.

Keywords: Multi-agent System, Software Architecture, Video Surveillance, Distributed Systems

1. INTRODUCTION

Intelligent visual surveillance systems deal with the real-time monitoring of persistent and transient objects within a specific environment. The primary aims of these systems are to provide an automatic interpretation of scenes and to understand and predict the actions and interactions of the observed objects based on the information acquired by sensors. With the development of sensor and network technology, multiple camera distributed surveillance system is considered mostly for video surveillance at present. Spatially distributed multi-sensor environments present interesting opportunities and challenges for surveillance.

The main stages of processing in an intelligent visual surveillance system are: moving object detection and recognition, tracking, behavioral analysis and retrieval. These stages involve the topics of machine vision, pattern analysis, artificial intelligence and data management. Most video content analysis algorithms are computationally intensive, the system requires a distributed computing environment to support real-time processing. Therefore, to integrate these algorithms into a working system and deploy them into a distributed environment remains a difficult problem that calls for a platform or architecture to support the distributed information processing and algorithms' integration.

Some new architectures and design methodology have been present in surveillance systems. Two surveillance systems, ADVISOR [1] and PRISMATICA [2], possess distributed architecture. Although both systems are classified as distributed architectures, they have a significant main difference in that PRISMATICA employs a centralized approach whereas ADVISOR can be considered as a semi-distributed architecture. PRISMATICA is built with the concept of a main or central computer which controls and supervises the whole system. This server thus becomes a critical single point of failure for the whole system. ADVISOR can be seen as a network of independent dedicated processor nodes (ADVISOR units), avoiding a single point-of-failure. Another architecture we have to mention is NeST (Networked Sensor Tapestry). It provides a test-bed for secure sharing, capture, distributed processing and archiving of surveillance data [3]. This architecture mainly emphasizes privacy. Due to the centralized nature, it faces problems of passing high-resolution video streams to remote clients. Another unsolved problem is data synchronization from various sensors, which is important in some applications like distributed camera handover.

In this paper, we present a multi-agent architecture for an intelligent distributed video surveillance system. All information processing module in intelligent distributed video surveillance application are encapsulated as agents. The architecture wrappers the real-time heterogeneous data share to simplify the modules' collaboration among agents.

The rest of the paper is organized as follows: In Section II, a multi-agent system architecture for the distributed surveillance systems is proposed. Collaboration among different agents is analyzed in Section III. Section IV presents an application of the system. Section V contains our conclusions and plans for future work.

2. SYSTEM ARCHITECTURE

The distributed surveillance systems include not only distributed array of cameras that offer wide area monitoring, but also a set of computer vision algorithms designed for scene analysis at multiple levels of abstraction [4]. For building an intelligent surveillance system, the system requires architecture for distributed computing environment to support real-time processing. The architecture has to be able to work in distributed environment, provides basic services and interface for all processing modules to collaborate, and is highly reliable and robust.

* This work was funded under Project 60672137 supported by the National Natural Science Foundation of China, Project 20060497015 supported by the Specialized Research Fund for the Doctoral Program of Higher Education of China, Project 2004ABA043 supported by the Natural Science Foundation of Hubei Province and Project D200612002 supported by the Key Scientific Research Project of Hubei Education Department.

The multi-agent concept is the basic technology of the overall communication infrastructure. The utilization of a multi-agent approach for intelligent distributed video surveillance application is reasonable due to the fact that agents are best suited for applications that are modular, decentralized, changeable, and complex [5]. The agent-oriented approaches can help in following ways. First, the modules developed by researchers to perform a special task can be easily encapsulated into agents and then imbedded in the platform to work. The whole system needs not to be well designed and carefully implemented before it can be deployed and tested. Second, as the agent base system is loose coupling, the agent can join or leave the environment freely, and the system would not likely to crash because of an agent's failure or leave.

The proposed multi-agent architecture can be expressed by a multi-level concept. The surveillance system can be divided in 4 different logical groups of tasks, in the following called level. The tasks that have to be performed within each level will be handled by one or several agents with different capabilities, as is illustrated in Fig. 1

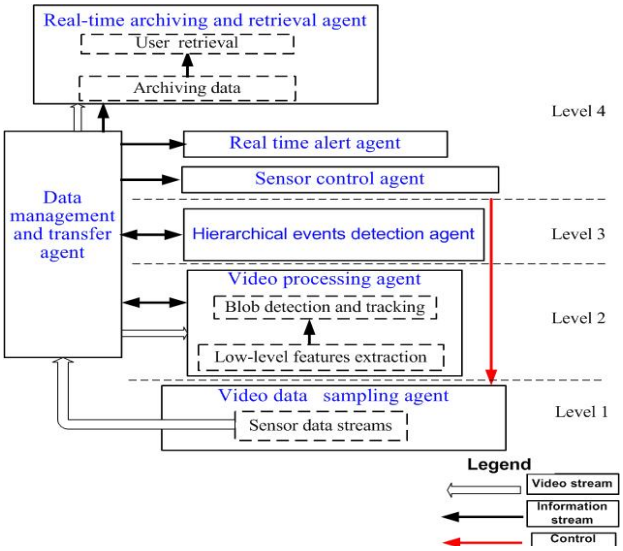


Fig.1. The multi-agent architecture for surveillance system

1) Level 1: Video data acquisition
   Video data sampling agent is responsible for video stream from multiple cameras connected by a Local Area Network (LAN) in level 1.
2) Level 2: Computer vision information processing
   The task of computer vision information processing is encapsulated as video processing agent that processes low-level features extraction and blob detection and extraction.
3) Level 3: Hierarchical events detection and recognition
   Hierarchical events detection agent recognizes and understands activities and behaviors of the tracked objects at different layer in surveillance system.
4) Level 4: Surveillance application
   Surveillance applications are performed by several agents, such as the real-time archiving and retrieval agent, the real-time alert agent and the sensor control agent. Real-time archiving and retrieval agent supports video retrieval that is based on the video index generated by automatic intelligent analysis. There are two types of alerts, user defined alerts and unusual activity alerts, can be generated by real-time alert agent. Sensor control agent is used to meet the current task of the system by controlling the movement and zoom of the cameras.

Data management and transfer agent is an important module that supports real-time heterogeneous data stream sharing and exchanging among agents in distributed surveillance system, which will be in detail discussed in next section.

3. COLLABORATION AMONG DIFFERENT AGENTS

3.1 Communication Content

Spatially distributed multi-sensor environments present interesting opportunities and challenges for surveillance. Recently, there has been some investigation of data fusion techniques to cope with the sharing of information obtained from different types of sensors [6]. The communication aspects within different parts of the system play an important role, with particular challenges either due to bandwidth constraints or the asymmetric nature of the communication [7].

In real-time intelligent distributed surveillance systems, there are various types of data to exchange between agents, including media data, metadata and control command, as listed in Table 1. Different types of data have different characteristic and transportation requirements. As a result, one of the major tasks of the architecture is to provide services for efficient sharing and exchanging of heterogeneous data by data management and transfer agent.

Table 1. Three information to exchange between agents

Type	Content	Data size	Linking number	Temporal continuity	Frequency
Control message	Command of controlling other modules to change status	Small	1	Sporadic	Little
Metadata	Data with semantics, and results of vision processing modules	Small ~Large	1, ...,n	Sporadic ~Continuous	Little ~Frequent
Streamed media data	Real-time video data streams	Large	0, ...,n	Continuous	Frequent

3.2 Communication Mechanism

We arrange all agents designed in intelligent distributed surveillance system in different hosts. As the hosts are connected with 100M Ethernet LAN, the TCP/UDP can provide appropriate performance. UDP is a suitable protocol for one-to-many communication without any buffer order problem in LAN, but it does not provide any congestion control. On the other hand, TCP provides a reliable one-to-one communication but not efficient for one-to-many communication. The TCP connections are built and maintained by all agents in different hosts. We are currently using a common config file to enable the agents to find each other and locate the resource.

We use MPEG-4 as our video CODEC, and the metadata and control message are created in a MPEG-7 compliant XML data structure. XML (Extensible Markup Language) is a simple, very flexible text format derived from SGML. XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere, which is originally designed to meet the challenges of large-scale electronic publishing. A communication that is based on XML language will be used whenever an agent wants to

communicate with one single or other agents.
Whenever an agent wants to supply information to several other agents or whenever there is a strong requirement to the processing speed, the communication will be based on the event mechanism. This represents the content of the messages as a XML document since it will be expressed as a String data type.

3.3 Synchronization of Streams

The distributed processing brings synchronization challenges that need be solved before the platform can work. This means this fusion application needs to synchronize different metadata which originate from different agents. We use both time and buffer symbol to synchronize the streams and metadata. When we got a compressed buffer from sensors, we add a buffer number and a time stamp to the head of the buffer. To synchronize streams from different hosts, an NTP (Network Time Protocol) server is set to ensure all camera workstations synchronized to a common time source.

4. APPLICATION

We implemented an intelligent distributed video surveillance system with a multi-agent platform. We use ACE framework to simplify the platform implementation and improve system robustness [8]. We also integrate an open source mpeg decode lib to decompress the mpeg streams produced by the capture card. We currently apply our platform as a test bed for the project that is based on intelligent meeting room and aims to create meeting archive in real-time.

5. CONCLUSIONS

Agent-oriented approaches have been proved to be efficient way for analyzing, designing, and implementing complex systems. It is reasonable to take advantage of the agent-based approaches to help designing intelligent distributed video surveillance system. Most video content analysis algorithms are computationally intensive, the system requires a distributed computing environment to support real-time processing. In this paper, we present a multi-agent architecture for an intelligent distributed video surveillance system. All information processing module in intelligent distributed video surveillance application are encapsulated as agents. The architecture wraps the real-time heterogeneous data into the data management and transfer agent to simplify the modules' collaboration among agents. We design various mechanisms for efficient delivery of different kinds of data streams.

The system is currently in its infancy. A lot tasks need to be done before a robust version could be released. However, for its advanced and open architecture, we believe it will play an important role in the researches and development of complex distributed real-time systems.

REFERENCES

[1] C.I.Attwood, D.A.Watson, "Advisor-socket and see: lessons learnt in building a real-time distributed surveillance system", *Intelligent Distributed Surveilliance Systems(IDSS-04)*, IEE, 23 Feb.2004 pp.6 – 11.

[2] A.Sergio, Velastin, Benny Lo, Jie Sun, "A flexible communications protocol for a distributed surveillance system", *Journal of Network and Computer Applications 27 ,2004*, pp.221–253.

[3] Douglas A. Fidaleo, Hoang-Anh Nguyen, Mohan Trivedi. "The Networked Sensor Tapestry (NeST): A Privacy Enhanced Software Architecture for Interactive Analysis of Data in Video-Sensor Networks". *International Multimedia Conference archive Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks*, pp.46 – 53.

[4] Valera, M. Velastin, S.A: "Intelligent distributed surveillance systems: a review. Vision, Image and Signal Processing", *IEE Proceedings-Volume 152*, Issue 2, 8 April 2005. pp.192-204.

[5] Parunak H. van Dyke., " Practical and Industrial Applications for Agent-Based Systems" , Industrial Technology Institute, 1998.

[6] Collins R.T., Lipton A.J., Kanade T. , et al: "A system for video surveillance and monitoring", Robotics Institute, Carnegie Mellon University, 2000, pp.1–68.

[7] Regazzoni, C.S, Ramesh, V, and Foresti, G.L.: "Special issue on video communications, processing, and understanding for third generation surveillance systems", *Proc. IEEE*, 2001, 89, (10), pp. 1355–1365.

[8] Stephen D. Huston, James CE Johnson, "Umar Syyid.: ACE Programmer's Guide", *The Practical Design Patterns for Network and Systems Programming.*

XiaoLing Xiao was born in 1973. She is an associate professor. She received the master's degree in institute of computer science and technology in Huazhong University of Science and Technology in 2002. She is currently a Ph. D. candidate in Computer Science of the Wuhan University of Technology. Her research interests include computer network and pattern recognition. She has published over 20 journal papers.

Layuan Li was born in 1946. He received the B. E. degree in Communication Engineering from Harbin Institute of Military Engineering in 1970 and the M.E. degree in Communication and Electrical Systems from Huazhong University of Science and Technology in 1982. He academically visited Massachusetts Institute of Technology (MIT) , USA in 1985 and 1999 , respectively. Since 1982 , he has been with the Wuhan University of Technology (WU T) where he is currently a professor and Ph. D. tutor of computer science , and editor in chief of the Journal of WUT. He is director of International Society of High-Technol. and paper reviewer of IEEE INFOCOM, ICCC and ISRSDC. His research interests include high speed computer networks , protocol engineering and image processing. He has published over one hundred and fifty technical papers and is the author of six books. He also was awarded the National Special Prize by the Chinese government in 1993.

Performance Analysis of the Parallel Particle Swarm Optimization Based on the Parallel Computation Models*

Yuanyuan Wang, Jianchao Zeng
Division of System Simulation & Computer Application,
Taiyuan University of Science and Technology,
Taiyuan 030024,Shanxi, China
Email:yuanyuan5219dong@126.com

ABSTRACT

The parallel programming based on the parallel computation models is a challenging subject for evolutionary computation algorithm. In the paper, the parallel particle swarm optimization (PPSO) algorithms are designed based on three parallel computation models which include parallel computation model with central controller, ring-structure model with buffer storages, and BSP parallel computation model. The performance has been analyzed and compared through simulation of two benchmark test functions. The experimental results show that the period of communication between microprocessors plays an important role for the performance of PPSO. If an appropriate period of communication is chosen, the quality of the solution can be improved besides the computer time is shortened.

Keywords: PSO, Parallel Computation Model, PPSO, Periodicity, Performance Analysis

1. INTRODUCTION

The Particle Swarm Optimization (PSO) was originally introduced in 1995 by Kennedy and Eberhart[1] and has been successfully applied to several different problems, including the training of neural networks, structural and topology optimization, image recognition, etc. PSO not only has some features of traditional EA (Evolution Algorithm) but also has many own favorable performance of optimization, such as very few parameters to adjust, simple and easy to program. During a few years Only, PSO develops rapidly and has formed a new research hotspot in the fields of evolutionary computation. However, when PSO solves the complex large-scale engineering optimization problems, it needs large numbers of particles and increased numbers of generations in evolution, which results in the enhancement of computation cost. So, the idea of parallel is introduced into PSO, which combines the higher speed performance of parallel machine with the inherence parallel of PSO. Then the PPSO algorithms are proposed, which not only distribute computation, but also use cooperative with multi-populations to reduce greatly numeric effort [2] and operation time. Separating population improves the quality of results[3] and advances the diversity of population.

In order to decrease the computation time with the increase of problem complexity, parallel PSO is a natural choice. In this aspects, some research works have been introduced in literature. Sub-populations and migration strategy are introduced to construct a PPSO[4]. Three different communication strategies according to the relationship of every parameter have been researched in Paper[5],and so on. PPSO algorithms have been successfully applied to biology[6] and system discrimination [7]. Anyway, PPSO research has important meaning, which has good computation effect in solving the large-scale engineer problems.

Parallel computation models are abstract[8] of the characters of parallel machine. Designing parallel algorithm cannot localize any concrete parallel machines, and must depend on nonobjective computation models. Now the three different PPSO are designed based on the three different parallel models. Many experiments show that parallel algorithms are efficient.

2. PARALLEL COMPUTATION MODELS

There are four typical models: master-slave, coarse-grain, fine-grain and hierarchy in parallel evolution algorithms. Because of lesser spending in communication time and better diversity of population, Coarse-grain models have been applied widely. This paper designs two different coarse-grain models and a BSP parallel model.

2.1 Parallel Computation Model with Central Controller

The model composed of N processors extends the PRAM (Parallel Random Access Machine). Every processor has local memory, clock and program. Central controller achieves communication, whose function is to compare the middle results periodically and update the best position (BP) and best fitness (BF). Every processor shares updated information. Fig.1 shows this model.

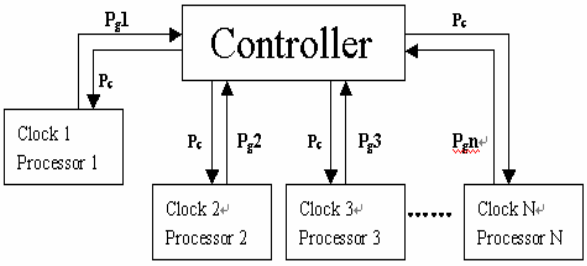


Fig.1. Parallel computation model with central controller

This coarse-grain parallel model can reduce the communication time efficiently and keep the characters of standard PSO.

2.2 Ring Structure Model with Buffer Storages

Through studying parallel computation models and enlightened by Parallel Genetic Algorithm (PGA), this section designs a ring structure with buffer storages model which is extension of island model. There are different connections between islands. Now this model is a ring topology, which assures that the best particle is diffused to all sub-populations and improves diversity of sub-populations. Fig.2 shows ring topology model.

* Key scientific research project fund of the ministry of education (204018)

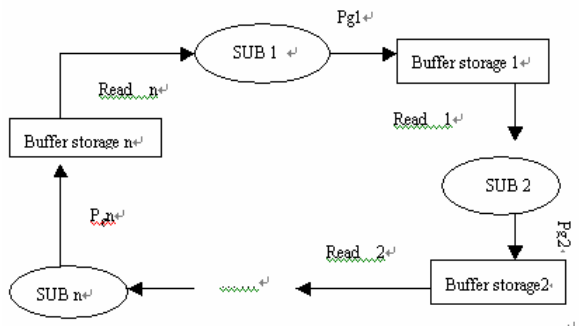


Fig .2. Ring topology model with buffers

2.3 BSP Parallel Model

A BSP computer is composed of n processors/storages connected with network. In BSP model, computation is made up of series supersteps that are synchronous and the period is L. Every processor executes local computation, receives and sends message by router in continued supersteps. Then the global checking makes sure whether all processors have accomplished this superstep. If all processors are finished, the computation goes to next superstep, or else the next L is given to the superstep that has not been accomplished.

BSP programs have n processes that stay in one node. Programs are executed according to the order of superstep strictly. In Fig.3 superstep uses synchronization barrier. Every superstep is divided into three parts showed by Fig.3.

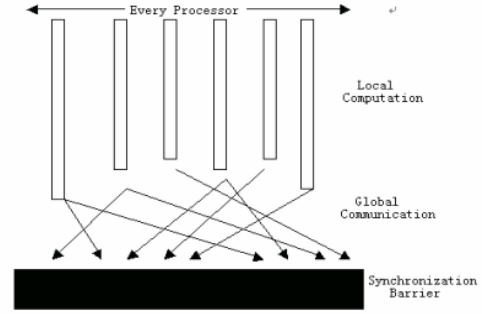


Fig.3. A superstep of BSP

Separation of computation task is the character of BSP, which simplifies the design and analysis. However, this way sacrifices the run time. The whole synchronism means that all the processes must wait the slowest one. Asynchronism has higher coupling and easily brings bottleneck of communication. This PPSO based on the BSP uses synchronization.

3. PPSO ALGORITHM

3.1 PPSO Based on the Parallel Computation Model with Central Controller (PPSO-controller)

Firstly, algorithm initializes the whole population and gets global best position (PG) and best fitness (F), which are shared information. Then it divides population into several sub-populations. Each sub-population runs in a process independently, which only updates own BP (Pg_i) and BF (f_i). When evolution generation is M, every sub-population puts current (Pg_i) and (f_i) into central controller. Through comparison, controller attains (PG) and (F) of the whole population which are shared information again. Every sub-population continues to evolve according to this shared information. Central controller attains new-shared information periodically. Algorithm is running in circle until a predefined maximum number of generations is met.

In fact, when M=1, it is a standard PSO. When M is greater than the maximum number of generations, every sub-population evolves independently, which has no introduction of PG. The algorithm cannot convergence. So the period of communication influences the performance of algorithm. In view of limited paper, here only selects part results of experiments to explain.

3.2 PPSO Based on the Ring Structure with Buffer Storages (PPSO-ring)

The algorithm divides the whole population into several sub-populations that run standard PSO independently. When generation is R(R is period), sub-population1 writes current BP (Pg_1) and BF($F(Pg_1)$) into buffer storage1. Then sub-population2 gets them from buffer storage1, which introduce the evolution of sub-population2. At the same time, sub-population2 writes current BP (Pg_2) and BF ($F(Pg_2)$) into buffer storage2. The sub-population 3 gets them from buffer storage2. Running goes along until sub-population n gets them from n-1 buffer storage which introduces the evolution of sub-population n. Sub-population n writes current BP (Pg_n) and BF ($F(Pg_n)$) into buffer storage n, from which sub-population1 gets them. Before writing the best fitness, algorithm estimates whether the current best fitness satisfies precision. If yes, algorithm stops or else the algorithm continues to evolve. Ever R generation, the neighbours of sub-populations communicate each other. Algorithm is running in circle until the precision is satisfied.

In this algorithm, every sub-population runs by turns. When the generation of sub-population is R, the Pg_1 introducing sub-population2 is passed to sub-population 2.When R is reached again, Pg_2 introduces the sub-population3, and so on. The neighbour gives next sub-population current BP that introduces the evolution. So particles can fly quickly into BP. Compared to PPSO-controller, PPSO-Ring improves the speed of convergence, which is approved by section 4.3.

3.3 PPSO Based on the BSP Model (BSPPSO)

Step1: Initialize a population that including many particles. Every particle has a random position and velocity. Compute the initial fitness, individual best location Pi and population's best location.

Step2: Divide the whole population into several sub-populations that evolve independently.

2.1 Every sub-population uses Pi, Pg to evolve according to evolution equation. Then compute the fitness of particles.

2.2 If one particle's fitness of some sub-population is better than Pg, it replaces the Pg. Other sub-populations continue to evolve according to this updated Pg, until the slowest sub-population updates the Pg.

Step3: Loop to step 2.1untill stop criterion is met, usually a sufficiently good fitness value or a predefined maximum number of generations.

Every sub-population uses individual BP and global BP to evolve independently according to evolutionary equation. Because of different pace, when the faster sub-population attains the best location current (Pg), Pg will influence other evolving sub-populations and introduce these particles to the best location, which can increase the speed of convergence.

3. SIMULATION EXPERIMENTS RESULTS AND DISCUSSION

The environment of simulation experiments is Windows and programming language is VC++6.0. The speed-up ratio is defined as T1/T2, in which T1 is the time of running standard PSO. T2=max (t_1,t_2……t_n) that is bad time. Running PPSO algorithm, the time of every sub-population is (t_1, t_2……t_n).

The times of reach best fitness (RBF) is defined as: in evolution, if the BF satisfies predefined precision, RBF is marked one time until evolution stop.

In this experiments, both standard PSO and PPSO select the same parameters and the same number of particles. Because of the randomicity of PSO, the results of experiment are average of 50 times running. Section 4.1,4.2 and 4.3 have the same testing function that is F2:Griewank function.

F2: $f_2(x) = \sum_{i=1}^{n} x_i^2/4000 - \prod_{i=1}^{n} \cos(x_i/\sqrt{i}) + 1 \quad -10 \le x_i \le 10$

4.1. PPSO-controller Results

The number of particles is 30 (n=30); the number of simulation processor is 3;every processor has 10 particles.

(1) Dimension is 100 (d=100); precision is 0.01; the number of evolution generation is 2000. Fig.4 and Fig.5 show the results.

Table 1. The results of griewank function (1)

Method	Period	RBF	Speedup ratio	Time
Standard PSO	——	5	——	4.68092
PPSO—Controller	1	5	2.979428	——
	10	32	2.981858	——
	20	36	2.982504	——
	50	36	2.932356	——
	100	37	2.976851	——
	200	27	2.965761	——
	500	0	2.94694	——
	1000	0	2.961221	——
	2000	0	2.985547	——

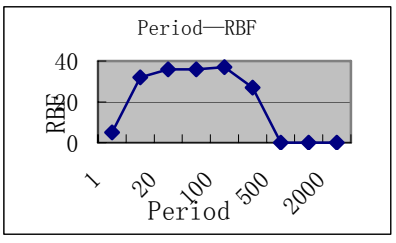


Fig.4. Period—RBF

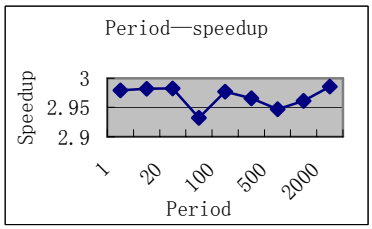


Fig.5. Period—Speedup ratio

(2) The number of particles is 100 (n=100); dimension is 100(d=100); the number of generation is 2000; precision is 0.01. Fig.6 and Fig.7 show the results.

Table 2. The results of griewank function (2)

Standard PSO	8	9.645600	——			
PPSO—Controller						
Period	Processor 3		Processor 7		Processor 10	
	RBF	Speedup ratio	RBF	Speedup ratio	RBF	Speedup ratio
1	8	2.602895	8	6.666759	8	9.906336
2	16	2.620745	8	6.69638	3	10.115713
5	25	2.580417	19	6.562704	17	10.007342
10	31	2.613601	33	6.619997	23	9.940322
20	34	2.601238	36	6.68793	18	10.028082
50	37	2.616324	19	6.546491	0	9.869159
100	29	2.560525	0	6.612282	0	10.056008
200	0	2.625582	0	6.626455	0	9.942365
500	0	2.622099	0	6.628458	0	9.894587
1000	0	2.405879	0	6.637307	0	10.035361

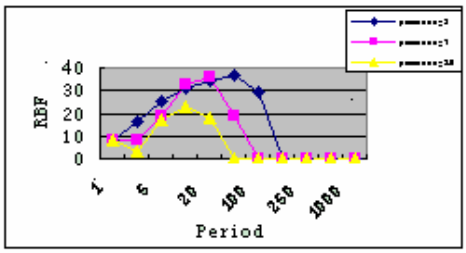


Fig.6. Period—RBF

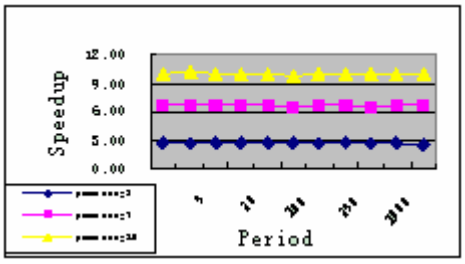


Fig.7. Period-Speedup ratio

The results show that the period of communication influences convergence. When R=1, both PPSO-controller and standard PSO have the same RBF. When T increased gradually, RBF changed greatly. For function F2, when R=20,50 or 100, RBF is 8 times than standard PSO. In a word, if an appropriate period is chosen, the convergence of this algorithm is good.

4.2. PPSO—ring Results

The number of particles is 100 (n=100); dimension is 100 (d=100); the number of generation is 2000;precision is 0.01. Fig.8 and Fig.9 show the results.

Table 3. the results of griewank function

Method	Period	RBF	Speedup ratio	Time
Standard PSO	——	5	——	4.74
PPSO—Ring	1	23	——	2.734534
	10	33	2.70674	——
	20	32	2.82651	——
	50	42	2.764083	——
	100	38	2.787055	——
	200	29	2.777517	——
	500	0	2.79943	——
	1000	0	2.82383	——
	2000	0	2.78401	——

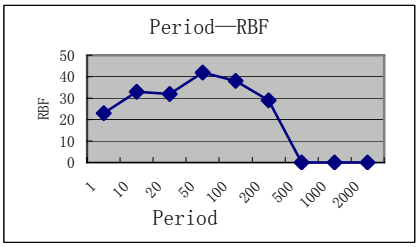


Fig.8. Period—RBF

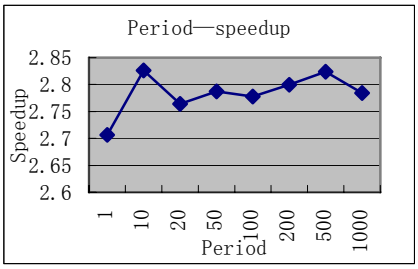


Fig.9. Period—Speedup ratio

The experiments show that the period of communication is very important. For F2, when the period is 50 or100, RBF is 9 times than standard PSO. It explains that periodical communication can build up diversity and improve the convergence.

The conclusion got from a lot of experiments is that the period has no influence on speed-up ratio, when experiments ignore the communication time. In this case, it is ideal state: speed-up ratio nearly equal to the number of processors, and the curve of figure changes smoothly. In theory, if the communication time is considered, period will influence the speed up ratio. When period is short, sub-populations have many communications that need a lot of time and the speed-up ratio is low. When period is long, sub-populations need a little communication that use a little time and the speed-up ratio is high.

4.3. Comparison of Results

The number of particles is 30 (n=30); dimension is 100 (d=100); the number of generation is 2000; precision is 0.01. The results are showed by Fig.10.

Table 4. Results of Griewank

Method	RBF	
Standard PSO	5	
Period（R）	PPSO—Controller RBF	PPSO—Ring RBF
1	5	27
2	11	24
5	18	21
10	26	36
20	36	35
30	38	41
50	36	39
100	34	34
200	0	0

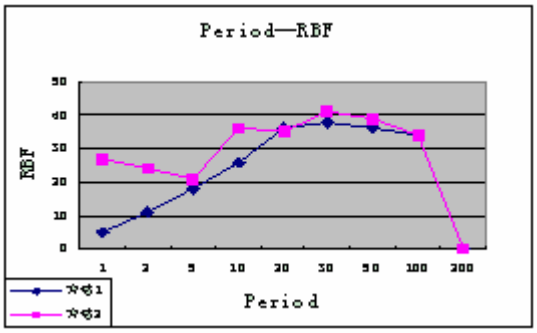


Fig.10. The results of comparison

As a whole, PPSO-Ring is better than PPSO-Controller according to the times of convergence, which can be seen clearly from Fig.10.

4.4. BSPPSO Experiment Results

The experiments use both standard PSO and BSPPSO methods for the tested unconstrained functions that are F1 sphere function and F2 Rosenbrock function. Compared the results, BSPPSO shows the better performance. The results are showed by Fig.11 and Fig.12.

Testing Function as follows：

F1: Sphere Function

$$f_1(x) = \sum_{i=1}^{n} x_i^2 \qquad -100 \le x_i \le 100$$

F2:Rosenbrock Function

$$f_2(x) = \sum_{i-1}^{n} (100(x_{i+1} - x_i^2)^2 + (x_i - 1)^2) \qquad -30 \le x_i \le 30$$

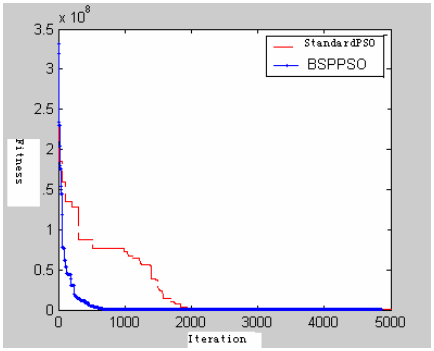


Fig.11. Sphere function

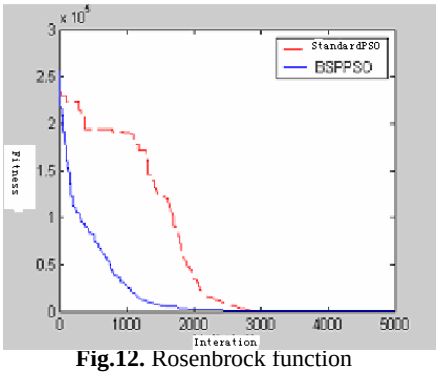


Fig.12. Rosenbrock function

Along with the increased number of generation, the changes of fitness in these two algorithms are different. Compared BSPPSO and PSO, BSPPSO has better convergence and fitness.

5. CONCLUSIONS

PPSO-Controller is synchronous, so all sub-populations have a same clock. It needs to be waiting until all the sub-populations reach the period. Then the shared information will be compared and updated. In PPSO-Ring, every sub-population has own clock, which doesn't need to wait. Neighbour appears current BP that introduces the next sub-population. So the convergence of PPSO-Ring is better than PPSO-Controller.

BSPPSO introduces BSP model into standard PSO, which changes the pattern of standard PSO. A new parallel PSO that may improve the search efficiency is designed based on BSP model. Compared BSPPSO and PSO, BSPPSO advances the performance greatly.

Parallel algorithm is an effective method for solving the complex large-scale engineering problems. A lot of experiments show that parallel algorithm can shorten the time, enhance the quality of results and improve the search efficiency.

REFERENCES

[1] J.Kennedy and R.C.Eberhart, "Particle swarm optimization," in Proc. IEEE International Conference on Neural Networks, Perth, Australis, Vol.4, 1995 PP. 1942-1948.

[2] Zeng Jian-chao，Jie jing，Cui Zhi-hua, "Particle swarm optimization," Beijing. Publisher of science，2004 (in Chinese).

[3] Xu You-zhun, Zen Wen-hua. "The Development Of Parallel Evolutionary Algorithms," *Pattern Recognition And Artificial Intelligence*,2005:18(2)(in Chinese).

[4] Zhao Yong, Yue Ji-guang, "A parallel particle swarm optimization algorithm based on multigroup for solving complex functions optimization," *Computer Engineering and Application*,2005:16(in Chinese).

[5] JUI-FANG CHANG,SHU-CHUAN CHU,JOHN F.RODDICK AND JENG-SHYANG PAN. "A Parallel Particle Swarm Optimization Algorithm with communication strategies," J*ournal of information science and engineering* 21,809-818(2005).

[6] J.F.Schutte,J.A.Reinbol,B.J.Fregly,R.T.Haftka,A.D.Georg e,"Parallel Global Optimization With the Particle Swarm Algorithm,"Int. J. Numer. Meth. Engng 2003.

[7] J F Schutte,B J Fregly. A parallel particle[C]. In: Proc 5th World Congress of structural and Multidisciplinary Optimization,Italy:Venice,2003：19-23

[8] Chen guo-liang, "Parallel Computation — Structure •Algorithm•Program". Publisher of high education, 2003 (in Chinese).

Yuanyuan Wang (1981-), female, was born in Yang Quan city of ShanXi province. She is a master graduate student. The main research interests are in swarm intelligence optimization algorithm and parallel computation.

Jianchao Zeng (1963-), male, is a professor, and the teacher of doctors. He is a vice president of Tai Yuan University of science and technology, and a head of computer science and technology school. His research interests are in complex system modeling, computation intelligence, simulation and optimization, etc. He has published over 180 papers, in which more than 100 papers have been embodied by SCI、EI.

Research and Implementation of Intelligent Autonomous Decentralized System*

Jiquan Shen [1, 2], Aizhong Mi [1, 2], Yixin Yin [2], Xuyan Tu [2]
[1] School of Computer Science and Technology, Henan Polytechnic University
Jiaozuo, Henan 454000, China.
[2] Information Engineering School, Beijing University of Science and Technology
Beijing 100083, China
Email: sjq0273@sina.com

ABSTRACT

Autonomous Decentralized System (ADS) is applied to control large system, management large system and information large system based on computer networks to resolve the problems of on-line expansion, on-line maintenance, etc, while Intelligent Autonomous Decentralized System (IADS) can improve the intelligence level and coordinating ability of ADS in order to meet the requirements of structure modifications and evolutions in actual large systems. Combining the architecture and design methods of IADS with the complicated production process and complex craft characteristics of medium and thick steel plate, an IADS for medium and thick steel plate tracking management is designed in two aspects, namely the system structure and software implementation. The highly real-time and stable system composed of many decentralized and autonomous subsystems can completely satisfy the demands of medium and thick steel plate production management and enhance the modern management level of the enterprise in the meantime.

Keywords: ADS, IADS, Network, Medium

1 INTRODUCTION

With the development of industry and computer technology, industrial manufacturing control and management systems are so perfect and large that single computer can hardly accomplish all tasks in a system. Although a large-scale computer is generally competent for that, its use has many constraints: hardware cost is high, system software and development software are not all-purpose, application software has a high development cost and maintenance is difficult. Generally, an industrial manufacturing control and management system consists of many autonomous and decentralized subsystems, so how to guarantee not only the independence and high processing performance of each decentralized subsystem but also a high speed and accurate communication between them in order to promote the coordination processing capacity of the whole system has become the key in the system design. Kinji Mori presented the Autonomous Decentralized System (ADS, see Fig.1), which is applied to control large system, management large system and information large system based on computer networks to resolve the problems of on-line expansion, on-line maintenance, etc.

This work is supported by China National Natural Science foundation (Grant No: 60374032)

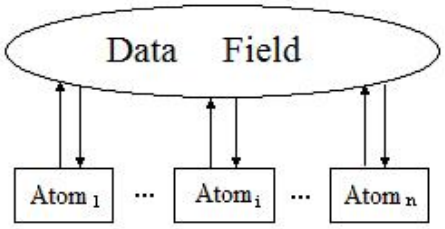


Fig.1. Autonomous decentralized system

ADS, a large system with decentralized structure, is composed of largely autonomous, decentralized and interrelated Atoms which exchange and share data through the “Data Field” (DF).

Atom: It corresponds to the software and hardware equipments of a node in computer networks. ADS supposes all Atoms satisfy such Self-Containment, Locality and Equality as conditions.

Data Field (DF): It’s a space for Atoms in ADS to exchange and share data, which corresponds to the public database and data communication network in computer networks. Its characteristics are as follows : Each data in DF is uniquely defined with respect to its content and accessed in class, and the data communications between the DF and Atoms follow Autonomous Decentralized Protocol (ADP).

ADS has the following features [1][7]:

1) Decentralized control structure: ADS is composed of many indirectly interrelated Atoms which exchange and share data through the DF. It has the basic structure characteristics of decentralized large systems: decentralized control, decentralized information and decentralized risk. As a result, the system has higher reliability and flexibility, but lower coordination.
2) Autonomous control characteristic: In ADS, each subsystem in different places has the property of “autonomous controllability” and its own local controller. It performs autonomous, decentralized local control respectively by its controller without being directed from the other subsystems. Hence, if any subsystem fails, is removed, is repaired, is updated technically or is expanded, the other subsystems can continue to manage themselves and to perform their own responsible functions. Consequently, the system satisfies the objectives of on-line expansion and on-line maintenance.
3) Autonomous coordination mode: In ADS, all of the subsystems are connected only through the DF, and just share and exchange data without mutual excitations and constraints. That is to say, each subsystem is still independent and autonomous controlled. This kind of decentralized coordination mode is called autonomous coordination mode, the essential of which is lessening coupling and autonomy.

Because it has higher reliability and flexibility as well as better

capability of on-line maintenance and on-line expansion, the ADS has been applied to computer control systems, computer management systems and computer information systems in railway transportation, industrial enterprises, etc. However, it has some problems need to be studied and resolved. Such as:

1) System structure problem: Actual decentralized large systems are not entirely and absolutely decentralized but partially and relatively decentralized. They have various structure modifications and evolutions. The assumption conditions about the Atom in ADS (Self-Containment, Locality and Equality) are hardly to be completely met in actual systems. So, ADS cannot meet the requirements of various structure modifications and evolutions in actual decentralized large systems.
2) Decentralized coordination problem: There are some conflicts between "Autonomy" and "Coordination". Each Atom in the ADS is autonomous, independent and locally controlled. The Atoms can't communicate mutually in a direct way, so there is no directly mutual excitation and constraint among them. They are just connected indirectly through the DF to share and exchange data. Thus, the lower coordination of ADS is a problem need to be resolved.
3) Intelligence level problem: Intelligence is the new trend, new stage of information-based and networked development. Artificial Intelligence (AI) is a new method, a new technique for the research and development of control system, management system and information system. But, the intelligence level of current ADS isn't high. How to apply Generalized Artificial Intelligence (GAI), especially the theories, methods and techniques of the Distributed Artificial Intelligence (DAI), to improving the intelligence level of ADS need to be studied further.

2 INTELLIGENT AUTONOMOUS DECENTRALIZED SYSTEM (IADS)

2.1 IADS Concept and Model

IADS[1][7] was presented in order to meet the requirements of structure modifications and evolutions in actual large systems. Its model is described as follows:

DAI + DCT + CNT → IADS

Where: DAI—Distributed Artificial Intelligence; DCT—Decentralized Control Theory; CNT—Computer Network Technology; IADS—Intelligent Autonomous Decentralized System.

IADS has not only the features of ADS but also the following features:

1) Coordination: In IADS, all of the subsystems realize cooperative operations and decentralized services by the mutual contacts, excitations and constraints among them.
2) Humanoid intelligence: IADS can be considered as the development based on the combination of ADS and Distributed Artificial Intelligence (DAI). It has not only the functions of autonomous controllability, autonomous coordination, on-line expansion and on-line maintenance, but also some humanoid intelligence, such as: activity, sensibility, reactivity, mobility, sociality, etc.

2.2 IADS Architecture

According to the "Structural Coordination" theory, the architecture of control system, management system and information system need respectively be coordinate and adaptive to the architecture of control object, management object and service object. Therefore, as the design scheme of decentralized control large system, decentralized management large system and decentralized information large system, the architecture of IADS ought to be coordinate and adaptive to the architecture of actual decentralized large system.

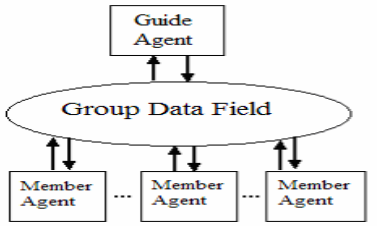


Fig.2. Group IADS

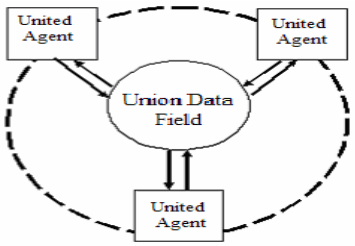


Fig.3. Union IADS

In the fields of engineering, social economy and ecological environment, the actual decentralized large system has not only "Entirely Decentralized" structure, but also various "Partial Decentralized" structure modifications and evolutions. In accordance with the design idea of IADS, two kinds of typical architecture of IADS are suggested as follows: Group IADS (GIADS, see Fig.2) and Union IADS (UIADS, see Fig.3).

In the GIADS, Guide Agent is the agent with guide function and corresponds to the superior management unit of the group. It is responsible for the global control and management of the group and performs "Guide Coordination" to Member Agents. Adopting the Guide Coordination strategy can strengthen the Guide Agent's decentralized coordination control to the Member Agents in the group, which is helpful to the group member's mutual coordination and cooperative operation. Member Agent corresponding to the inferior member unit is responsible for the local control and management of the group and accepts the management and coordination control from the Guide Agent. Group DF corresponds to Intranet and the public database of the group. In the group, "Multi-Bases Cooperation" technique is adopted, each data is uniquely defined with respect to its content and managed in class, and access control in accordance with the member authority is also introduced. All the Member Agents cannot only exchange and share data through the Group DF, but also communicate mutually, operate cooperatively and receive Guide Coordination orders from the Guide Agent through the Intranet. The Group DF has data security measures to keep "hackers" outside the group from invading, to avoid the interference of "virus", and to guarantee the data reliability and the credibility of data sources. The GIADS achieves the "Central-Decentralized" distributed intelligence through the combination of the Guide Agent and the Member Agents. It adopts the Guide Coordination strategy as well as negotiation, cooperation, and coordination methods, techniques of Multi-Agent System. Each Member Agent has local decentralized "autonomous controllability" and "autonomous coordination" and the Guide Agent has the global centralized functions of optimization and coordination control make the system have a higher intelligence.

In the UIADS, United Agent is the autonomous decentralized

subsystem that has joined the union and each United Agent hasrelatively autonomy and equality. The United Agent has local control and management function and its own LAN (Intranet based on Web technology). In the mean time, all of them follow collective "Union Protocol". Each United Agent gets excitations from the union and also accepts the constraints of the union. In accordance with the Union Protocol, the UIADS can adopt "Hologram Coordination" or "Circulation Coordination" strategy. Through the distributed Union DF, the United Agents cannot only exchange and share union data, but also communicate mutually in a direct way. Each United Agent has stronger decentralized coordination ability in order to realize the cooperative operation of the union. The Union DF corresponds to the Extranet among the United Agents and the distributed union databases. The United Agents can exchange, share data, and communicate mutually in a direct way according to the Union Protocol. The "Hologram Coordination" strategy as well as negotiation, cooperation, and coordination methods, techniques of the Multi-Agent System can be adopted to perform the mutual coordination among the United Agents in order to realize the cooperative operation of the union.

In the design and development of IADS, many methods and techniques have to be introduced, such as Distributed Artificial Intelligence (DAI), Decentralized Control Theory (DCT), Computer Network Technology (CNT), etc.

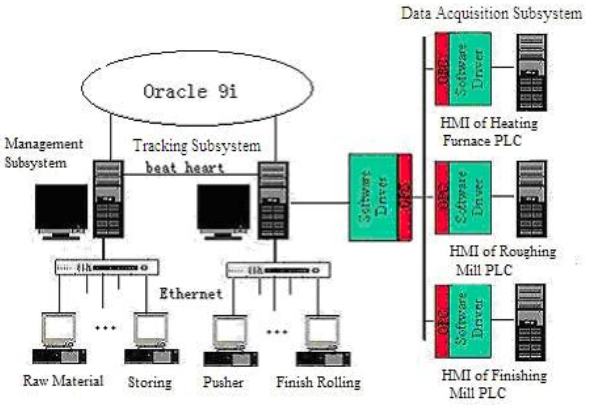


Fig.4. The topology of the IADS for the tracking management of medium and thick steel plate

3. THE IADS FOR THE TRACKING MANAGEMENT OF MEDIUM AND THICK STEEL PLATE

3.1 System Topology and Primary Functions of Each Subsystem

According to the craft characteristics of medium and thick steel plate, an IADS for the tracking management of medium and thick steel plate was established, and Fig.4 is its topology [2-6][8]. The system consists of a tracking subsystem, a management subsystem and a data acquisition subsystem, and three subsystems are connected mutually through high-speed Ethernet. The OPC Clients of the tracking and the data acquisition subsystem synchronously run on the tracking server. The data acquisition subsystem is composed of three terminals of "the HMI of PLC" and the tracking server. Three terminals of the "HMI of PLC" are as the OPC Server of the data acquisition subsystem and the tracking sever is as the OPC Client in the mean time.

(1) Tracking subsystem: It is oriented to the production process control, accomplishes the logical judgments of slab tracking (Presently, the Second Rolling Plant of Anyang Iron and Steel Company adopts two-stand four high reversing mill, whose tracking logic is more complicated than that of single-stand four high reversing mill), and implements the tasks of slab position tracking, data scheduling, control, etc. It is the key of the whole slab quality tracking management system of the medium and thick steel plate's production line. Only correct tracking can guarantee the normal operation and function implementation of the whole system. The main purpose of tracking is to make the computer know each slab's actual craft position and control state in the rolling production line in order that the computer can start relevant function programs to control the corresponding slab accurately, to deal with the sampling of related data, to guarantee the slab's normal rolling and to avoid accidents. There are many slabs on the rolling production line at the same time, and not only each slab's rolling state is different, but also the slabs may diverse from each other in specification and type. Thus, besides the actual craft position of each slab is tracked, the data of each slab is stored into the corresponding database in company with the change of its actual craft position [3].

(2) Management subsystem: It adopts a hybrid structure combing C/S and B/S, and mainly includes the management of raw material, finished product, production technique index, etc:
* The raw material management is mainly responsible for handling raw materials, production program and production card data, and includes raw material data's recording, modify, delete, query, and statistics; production program's establishment, modify, delete, query, and statistics; production card's issuance.
*The finished product management mainly accomplishes the functions of automatically computing each finished product's weight and the total weight each pile, etc. In addition, it can perform the processes of throwing steel, throwing steel recovery, back-cut and discard, etc.
* The management of production technique index can provide the query by work shift, type of steel, and specification, and automatically generate the production daily, monthly and annual.

(3) Data acquisition subsystem: It collects the necessary control signals and related data for the other two subsystems from the PLC, and transfers the gathered data to the tracking subsystem by OPC (OLE for Process Control). The OPC is designed according to the COM/DCOM technique, which normalizes the software interface standard in the field of industrial control and provides two interface schemes, namely custom interface and automation interface. The data acquisition subsystem is composed of three OPC Servers and one OPC Client.

3.2 Key Problems in the System Design

Three subsystems in the system are autonomous and decentralized, so coordination control are required to guarantee the cooperative operation of the system [2][6].

(1) Autonomy: The subsystems are autonomous computer systems, and all of them can run synchronously and independently as long as their operating conditions are satisfied. Here need particularize that dividing the whole system into three autonomous subsystems instead of a large system is mainly owing to the following factors: First, the data acquisition subsystem is close correlative with the PLC on the spot and mainly responsible for

collecting the corresponding control signals and related parameter data (e.g. rolling force, twisting moment, roll gap, etc). Its functions are relatively independent, so it becomes a system solely. Second, the tracking and the management subsystem ought to be designed as one system, but the tracking subsystem tracks the slab's position according to the corresponding control signals gathered by the data acquisition subsystem and controls the data movement accordingly. Once it can't work for a certain reason (e.g. failure of detecting elements on the spot, network failure, etc) and the production of the spot don't stop at this time, the management subsystem must work independently for the sake of the consistency and integrity of data. Consequently, the storing management of the management subsystem must have two kinds of work modes, and one is acquiring data from the tracking subsystem (when the tracking subsystem is working normally), the other is directly acquiring data from the raw material management of the management subsystem (when the tracking subsystem can't work).

(2) Real-time: In the OPC, the efficiency of the custom interface is higher than that of the automation interface, so Visual C++ language is adopted to develop the application program of the OPC Client. The subsystems are connected through Gigabit Ethernet, and the communication medium adopts fiber optic, whose high data transfer rate can guarantee the communication speed among the subsystems. The tracking subsystem is the core of the whole system and its task is the heaviest. Its main thread generally has a long operational cycle, which is certain to influence the real-time response speed of the whole system. So some relatively independent functional modules of it are designed as production threads in order to dramatically improve the real-time response ability of the system. Four production threads are developed: pThread[0] is responsible for the data acquisition and the tracking logical control in the furnace's frontal area, whose format is "pThread[0]= AfxBeginThread(ThreadProc0, GetSafeHwnd(), THREAD_PRIORITY_NORMAL)", where the format of the function ThreadProc0 is "UINT ThreadProc0(LPVOID pParam)".
pThread[1] is in charge of the data acquisition and the tracking logical control of the roughing mill; pThread[2] is in charge of the data acquisition and the tracking logical control of the finishing mill; pThread[3] is in charge of the data acquisition and the tracking logical control of the straightening machine as well as handling the data exchange between the tracking and the management subsystem.

(3) Cooperation: To guarantee the cooperative operation of three subsystems, between the tracking and the management subsystem, the subscription mode is chose from three kinds of data access mode of OPC (synchronous, asynchronous, subscription). In the subscription mode, the OPC Client doesn't have to send requests to the OPC Server, while the OPC Server automatically informs the OPC Client in a certain update cycle. The tracking and the management subsystem exchange data through the Oracle 9i database and the trigger technique of the database is mainly adopted to achieve the cooperative operation of two subsystems.

(4) synchronous and asynchronous: Three subsystems have some parallel features including independence, synchronization, etc. The execution results of each subsystem are the execution conditions of the other two subsystems, and three subsystems share the same data area and some other resources. Therefore, the synchronization and mutual exclusion problem among subsystems need be resolved. In the system, corresponding flag word or flag bit of flag word as well as locking critical region are mainly adopted to resolve this problem.

(5) Intelligence: The management subsystem adopts the Intelligence Information Pushes-Pull technique to make the whole management system have a high timely feature, a broad service range, a strong pertinence, and individual friendly services.

4. CONCLUSIONS

The above intelligent autonomous decentralized architecture has been applied to the slab quality tracking management system of the medium and thick steel plate's production line in the Second Rolling Plant of Anyang Iron and Steel Company. The practice shows the whole system has a rapid and accurate data communication, comprehensive functions and a stable performance. The system completely satisfies the demands of medium and thick steel plate's production management, enhances the production benefit and management level of the plant and speeds up the modern management process of the enterprise.

REFERENCES

[1] Tu Xuyan, Wang Cong, Guo Yanhui. *Large Systems Cybernetics*[M]. Beijing: Beijing University of Posts and Telecommunications Press,May 2005.

[2] Shen Jiquan, Tu Xuyan. "Research and Implement of Process Control System based on Parallel Computing"[J]. *Metallurgical Industry Automation*,Apr 2005,pp.48-50

[3] Jia Zongpu, Shen Jiquan. "The Design of the MediumandThick Steel Plate's Computer Process Control System"[J]. *Computer Engineering and Applications*, 2004.19,pp.206-208.

[4] Shen Jiquan, Wu Minfei, Ju Zhigang. "The Design of Sequence Control Subsystem of the Medium and Thick Steel Plate's Computer Control System"[J]. *Journal of Jiaozuo Institute of Technology*,Mar 2003,pp.147-150

[5] Sun Benrong et al. *Production of Medium and Thick Steel Plate*[M],Beijing: Metallurgical Industry Press,Jan 1993.

[6] Shen Jiquan, Wu Minfei,"The design of track subsystem of the medium and thick steel plate's computer control system"[J],*Journal of Jiaozuo Institute of Technology*, Mar 2002,pp.130-132.

[7] Tu Xuyan, Tang Tao. "Intelligent Autonomous Decentralized System (IADS)". *Proceedings of the 2nd International Workshop of IEEE Computer Society on Autonomous Decentralized*,Dec 2002,pp.10-15

[8] Zheng Xuefeng. "Integration Technology of Steel Rolling Computer Control System"[J]. *Metallurgical Industry Automation*,Mar 2001,pp.6.

FLASH：A Dependable Networked Data Storage Solution *

Ming Hu, Minghua Jiang
College of Computer Science, Wuhan University of Science and Engineering
Wuhan, HuBei Province 430073, China
Email: stereotype@263.net, mhjiang@126.com

ABSTRACT

To the depth of applying the Internet, information security has associated with the dependability of access platform, access path, and storage. The quality of dependable service focuses on controllability of accessing efficiency, availability, and security of application data. FLASH is proposed for dependable networked data storage systems in which new i-node structure is used to implement user's choices for file layouts such as non-stripping, non-striped mirroring, stripping, and striped mirroring and for security types such as fully sharing, releasing-with-signature, encrypted protection, and replicating protection. The solution provides the three-level dependable mechanism and functional agents implemented by clients, data servers, and object-based storage devices, and isolates user hosts from networked data storage both for users to select the proper quality of dependable service according to file content and access path and to guarantee the performance optimization of distributed storage systems.

Keywords: Data Storage,Dependable Network,Quality of Dependable Service

1. INTRODUCTION

Accessing data across the Internet is at the any time possible to confront the various manual and natural attacks which happen to platforms, paths, and storage devices of information accessing and affect the accessing efficiency, availability, and security of application data, so the information security of computer system has three aspects: system security, network security, and storage security. At present, much research on storage is to improve the quality of dependable service based on these three aspects.

Recently solutions of storage level improved both the accessing efficiency and the availability of storage systems by disk arrays[1-4]. Moreover, distributed storage systems can enhance network protection of data-accessing requests against manual attacks[5-8]. Their key problem is to improve just the quality of dependable service customized for the entire storage system or its one zone. Actually, different files have different requirements. Thus, the intrusion detection system for SAN[5] translated file-protecting rules into storage block-protecting ones.

Zhou JingLi and at al[9] presented the file-level method to optimize the accessing performance of file requests with different size. Based on this and for protecting storage systems from the manual and natural attacks, a dependable networked data storage solution, file-level agents of storage hierarchy (FLASH) provides the alternatives of data layout and security of file level for users and is implemented by a dependable data storage architecture where a client application is used as a security agent of user's file data, data server as a management and allocation agent of storage system, and object-based storage devices as accessing agents of file data. At last, we show that the three-level agents co-work to guarantee both users' quality of dependable service and the performance optimization of storage systems.

* Project Supported By HuBei Natural Science Foundation under Grant NO.2004ABA015 and Hubei Education Foundation under Grant NO. 2004D009.

2. DATA PLACEMENT AND SECURITY OF FILE LEVEL

Users need controllability of data-accessing efficiency, availability, and security to acquire different quality of dependable service according different data contents and user demands. Storage-level solutions are transparent and make a storage system looks like to user a single disk which only determines the data placement and security mechanism to optimize performance, availability, and security requirements related to storage. However, file-level solutions are not transparent to user. The metadata structure of data and the storage system determine together the data placement and security mechanism to optimize the data-accessing efficiency, availability, and security according to file content. Therefore, we tend to apply file-level solutions.

For controllability of data-accessing efficiency, availability, and security according to different data contents, it is necessary to take multiple storage devices as file-level entities. Without loss of generality, supposed that there are G object-based storage groups (OSGs) OSG_0, OSG_1, …, OSG_{G-1} and the i-th ORG has D object-based storage devices (OSDs) $OSD_{(i,0)}$, $OSD_{(i,1)}$, …, $OSD_{(i,D-1)}$ such that $OSG_i=\{OSD_{(i,0)}, OSD_{(i,1)}, \ldots, OSD_{(i,D-1)}\}$. As with non-stripped data distribution in NFS, all the data of a file are stored on the same OSD device and different files can be stored on different OSD devices. File i-node structure needs descriptor IOSG (0~G-1) for OSG group, IOSD (0~D-1) for OSD device, and iNumber for i-node. Like traditional file system, it maps logical addresses to storage locations of 4 bytes on the single OSD applying the allocation strategy of storage block with B(KB). Because of the limit of i-node structure, each file has at most C blocks with the logical data of C×B(KB) by direct addressing. If file is greater, it needs single-indirect addressing.

For one-level indirect addressing, a single-indirect address in i-node points to a pointer block in which each 4-byte points to the location of a data block. It has the addressing overhead of B(KB) and the addressing range of $(1/4)B^2$(MB). If the number of bytes in a file exceeds $C\times B(KB)+(1/4)B^2$(MB), it needs double-indirect addressing.

Similarly, two-level indirect addressing has the addressing overhead of $B(KB)+(1/4)B^2$(MB) and the addressing range of $(1/4)^2B^3$(GB). Therefore, the total addressing overhead is $2B(KB)+(1/4)B^2$(MB) and the maximum of file bytes is $C\times B(KB)+(1/4)B^2(MB)+(1/4)^2B^3$(GB). The early UNIX file system adopted the three-level indirect addressing because B=1/2. its total addressing overhead is

3B(KB)+(1/4)B^2(MB)+(1/4)$^2B^3$(GB) and the maximum of file bytes is C×B(KB)+(1/4)B^2(MB)+(1/4)$^2B^3$(GB)+(1/4)$^3B^4$(TB).
For such a file system implemented on single storage device, the storage volume can be expanded by disk arrays, such as RAID0. Because of 4-byte storage address, the maximum of storage volume is 2^{32}B(KB)=4B(TB). Generally, B=1/2~8 so it is 2~32(TB). In addition, for indirect addressing files, the number of indirect addressing levels determines the storage-accessing efficiency. Direct addressing data needs one time to access the storage while two-level addressing data need three times to access the storage.

The above non-stripping distribution can only implement the data parallel between different files. To implement the data parallel in a file, the file data need to be stripped across multiple storage devices applying the allocation strategy of storage segment as a stripe unit of S(KB) generally such that S≥16. Likely, descriptor IOSG is for an ORG group to apply stripping and descriptor IOSD for the OSD device to store the first segment and iNumber for i-node. File data has the maximum of C×S(KB)+(1/4)S^2(MB)+(1/4)$^2S^3$(GB) including C×S(KB) by direct addressing, (1/4)S^2(MB) and (1/4)$^2S^3$(GB) by one- and two-level indirect addressing respectively and its total overhead is 2S(KB)+(1/4)S^2(MB) including S(KB) and S(KB)+(1/4)S^2(MB) for one- and two-level indirect addressing respectively.

However, the computation of address, especially two-level addressing pointer, is quite complex because different addresses of 4-bytes may point to the storage locations on the different OSD devices. The computation needs to consider not only the number of data bytes in a file but also the addressing overhead of storage. Supposed IOSG is associated with OSG_i={$OSD_{(i,0)}$, $OSD_{(i,1)}$, …, $OSD_{(i,3)}$} and IOSD with $OSD_{(i,1)}$. As is illustrated in fig.1, the first segment is on $OSD_{(i,1)}$, the second segment on $OSD_{(i,2)}$, the fourth segment cyclically on $OSD_{(i,0)}$. At the time indirect addressing starts with the pointer segment, it needs to be expanded to data segment.

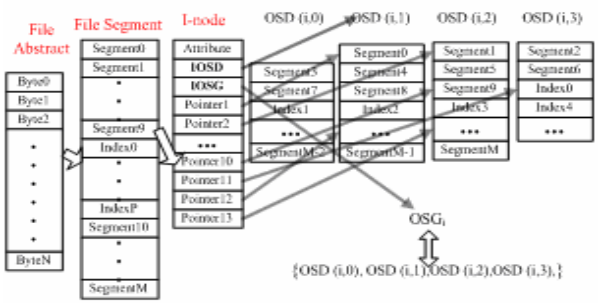


Fig.1. File-level striping structure

In general, bit maps are used for describing the used (set to 1) or free (set to 0) flags for storage blocks, so one byte is associated with the allocation of 8 blocks. In contrast with link list, bit maps tell the physical layout of storage and have the lower storage overhead (U/(8B))(MB), where U is storage volume in GB, B is block size in KB. Depending on disk-positioning overhead and network latency, small files are available for non-striped distribution and large files for striped distribution. Combining storage block allocation with segment allocation, S=8mB is useful to allocate m bytes for a storage segment, where B=4 and m=4, namely S=128 in this solution.
Descriptors IMOSG, IMOSD, and IMNumber have the same meaning as IOSG, IOSD, and INumber for mirroring of non-striped or striped file data. A file's i-node and i-node of its mirrored data are stored on the IOSD device and the IMOSD device respectively. These i-nodes need two bit field LTD to define layout type: 0 for non-striping (raw distribution), 1 for non-striped mirroring (file RAID1), 2 for striping (file RAID0), and 3 for striped mirroring (file RAID10). Address pointers in i-node can point to a storage block or a storage segment depending on layout types, where there are C direct addressing pointers (DA_0~DA_{C-1}), 1 single indirect addressing pointer (SIA), 1 double indirect addressing pointer (DIA). Therefore, the sequence (LTD, IOSG, IOSD, IMOSG, IMOSD, INumber, IMNumber, DA_0~DA_{C-1}, SIA, DIA) determines the layout structure of a file data. To thwart manual and natural attacks, directory file as a small file is non-striped mirroring distribution by default. The directory tree with its mirrored tree forms a shadow directory tree from the root directory.

For the security of file data, i-node needs a two-bit field STD to define the security type: 0 for fully sharing, 1 for releasing-with-signature, 2 for encrypted protection, and 3 for replicating protection. It still needs to add a field SPI for security parameter index. The fields STD and SPI determine together if security information field SI is added to file or directory data.

1) STD=0 means that a file or directory can be completely shared without SI;
2) STD=1 means that SI is encrypted message digest from a file or directory by its creator and is authenticated by sharers;
3) STD=2 means that logical data is the encrypted file or directory data by its creator and is only accessed by creator without SI;
4) STD=3 means that logical data is the encrypted file or directory data by symmetrical key which is encrypted into SI by creator applying the designated sharer's public key in order to copy the file or directory by the sharer.

FILE-LEVEL AGENTS OF STORAGE HIERARCHY FLASH

As is illustrated in Fig.2, the dependable networked data storage architecture provides file-level agents of storage hierarchy FLASH to implement the above file-level layout and security against manual and natural attacks. FLASH constructs physically a hierarchical dependable accessing mechanism: clients, data servers, and object-based storage devices, and logically a security-hierarchical accessing path: root directory, directories, and files.

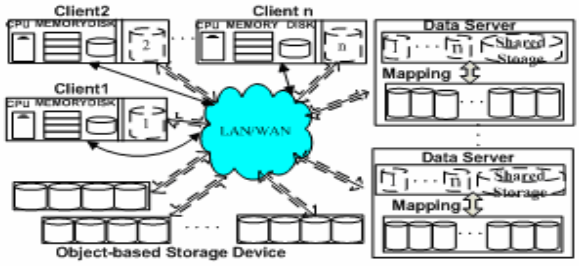


Fig.2. Dependable Networked Data Storage Architecture

Clients undertake missions as follows.

(1) Install correspondent file-accessing platform to take local disks as the portion of cache for file operations;
(2) make bidirectional authentication with data servers to acquire the ephemeral OSD-accessing rights to access files or directories;
(3) encrypt or decrypt user's data by symmetrical cryptography to access the files or directories with encrypted protection;
(4) authenticate data by applying the public keys of their creators or by applying user's own private keys

asymmetrically to SI field for files or directories with releasing-with-signature;
(5) for a file or directory with replicating protection, as a creator, encrypt it into shared area by applying a symmetric key which is encrypted by sharer's public key to SI field or as a sharer, move it into users' private area and decrypt SI field to acquire the symmetric key which is used to decrypt the file or directory;
(6) select the file layout type by open mode but the change of its layout type is completed and responded by data servers.

Data servers complete missions as follows:
(1) Provide security services between clients and OSDs or between OSDs and file-level intrusion detection mechanism, and help clients to find the root nodes and to do other metadata services;
(2) configure the storage system by OSD devices each of which is divided into multiple storage zones by partitioning and participate in an ORG group as a storage zone and assign multiple OSD devices to ORG groups according to the storage space balance and mirroring requirements that two ORG groups for mirroring have no shared OSD devices.
(3) assign an OSG group and OSD device, allocate and free the storage space for creating, deleting file or changing file layout to guarantee the balancing of used storage space and the pieces of segment allocation for block allocation.

OSD of a file's i-node points to an OSD device on which the file's i-node, all the file data for non-stripping layout or the first segment of the file data for stripping layout is stored. This OSD device acts as the dependable storage controller for the file, a file-accessing agent, and has the functions as follows.
(1) acts as the main storage controller associated with IOSD with the support of data servers for the root nodes, directories, files or as the slave storage controller associated with IMOSD if the main storage controller fails.
(2) completes the operations of file requests according to the information of the file's i-node, collaborates the data transmission between client and other OSD devices in the ORG group for stripping layout, or transfers its control to the OSD device associated with IMOSD if necessary.
(3) collaborates the data transmission between OSD devices in two ORG groups for striped mirroring based on the communication with the OSD associated with IMOSD.

3. CONCLUSIONS

FLASH presents a dependable networked data storage solution to protect user's data from manual and natural attacks. Data servers make use of security protocols for security accesses between physical devices such as clients, data servers, and OSD devices so that the storage of users' data are only accessed through their identities and isolated securely from the hosts used. A file's i-node designates the object-based storage group for storing the file data and the object-based storage device for accessing file data. Therefore, the access from the root of the file system to the user's directory to its file data is made from data servers and a sequence of OSD devices. They form a physical trust chain whose root is a data server.

File i-node structure provides the four security choices of fully sharing, releasing-with-signature, encrypted protection, and replicating protection. Users make use of the security directories or files provide, to implement a hierarchical security accessing mechanism for logical data. Users answer for the security problems of their data and data access by applications on clients while data servers make the intrusion detections based on file level. All these have no influence on the performance of the storage system.

The allocation of the ORG group and OSD device for a file is based on the strategy of balancing the used storage space and each OSD device joins an ORG group as a storage zone, so a massive OSD device with higher storage density and speed may participate in multiple ORG groups. Thus, the entering and leaving of a storage device have the less impact on the performance. It is easy to decentralize the control of storage devices, to dynamically balance the storage access and to form the hetero-storage system for the scalability and upgrading of the storage system.

File i-node structure provides the four layout types of non-striping, non-stripped mirroring, striping, and striped mirroring to select according to data size and access requirements. Users answer for the storage layout of their file data, data servers implement the two-level storage allocation of storage block and segment, and the OSD device designated by the file i-node responds the access and the storage mapping of the file data requests. Whether files are small or large, they have the same access efficiency and their storage locations are not affected by others' as in solutions of storage level. In addition, the block of 4KB and the segment of 128KB reduce the impact of indirect addressing and file fragments on the performance. For example, most of MP3 files can directly access by striping. In the case of concurrent file accessing, an OSD device can improve the disk-accessing efficiency by coalescing multiple address-consecutive data-accessing requests into a single one.

REFERENCES

[1] Plank J S,Xu Lihao,"Optimizing Cauchy Reed-Solomon Codes for Fault-Tolerant Network Storage Applications[C]," *Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications* (NCA '06),IEEE Computer Society, 2006,pp.173-180.
[2] Hafner J L,WEAVER Codes: "Highly Fault Tolerant Erasure Codes for Storage Systems [C]," *Proceedings of the 4th USENIX Conference on File and Storage Technologies* (FST'05),USENIX Association, 2005,pp.211-224.
[3] Hafner J L. "HoVer Erasure Codes For Disk Arrays[C]." *Proceedings of the International Conference on Dependable Systems and Networks (DSN'06).* IEEE Computer Society, 2006, Volume 00,pp.217-226.
[4] Hu Ming, Jiang Minghua. "RAID5x: A Performance-optimizing Scheme against Double Disk Failures." *Proceedings of 2006 International Symposium on Distributed Computing and Applications for Business, Engineering, and Science* (DCABES 2006).Shanghai University Press, 2006,Volume II,pp.1060-1063.
[5] Banikazemi M, Poff D E and Abali B. "Storage-based Intrusion Detection for Storage Area Networks (SANs)." *Proceedings of the 22nd IEEE / 13th NASA Goddard Conference on Mass Storage Systems and Technologies (MSST'05).* IEEE Computer Society, 2005, Volume 00,pp.118 - 127.
[6] Naor D, Factor M, Nagle D, Riedel E and Satran J. "The OSD Security Protocol." *Proceedings of the Third IEEE International Security in Storage Workshop (SISW'05).* IEEE Computer Society, 2005, Volume 00,pp.29 - 39.

[7] Liu Zhaobin. "Dependable Data Computing for Distributed System." *Proceedings of 2006 International Symposium on Distributed Computing and Applications for Business,Engineering, and Science*(DCABES 2006),Shanghai University Press,2006,Volume,pp.133-136

[8] Mitra S, Hsu W W, and Winslett M. "Trustworthy Keyword Search for Regulatory-Compliant Records Retention." *Proceedings of the 32nd international conference on Very large data bases (VLDB'06)* . VLDB Endowment, 2006, Volume 32,pp.1001-1012.

[9] Zhou JingLi, Hu Ming, and Yu ShengSheng. "The File System Implementation Method to Improve the Network Storage Performance."Mini-Micro Systems, 2006, 27(3), pp.396-400.

The Architecture of Workflow on Event Mapping Mechanism

Xin Li[1, 2]
[1]Department of Computer Science, Shantou University, Shantou, Guangdong, 515063, China
[2]The Key Laboratory of Intelligent Manufacturing Technology, Ministry of Education (at Shantou University)
Shantou, Guangdong, 515063, China
Email: lixin@stu.edu.cn

ABSTRACT

Workflow is a kind of advanced network service. It's considered that the procedure logic may be separated from the profession logic in workflow. However, that idea hasn't been carried out fully in its development. Instead, workflow is often looked upon in the view of the application. As result, many flexible methods, which are all application oriented, are presented to cope with troubles of the separation of procedure logic from profession logic. It makes workflow bound with concrete profession in fact. Obviously, that phenomenon is opposite to the original intention of workflow. Its idea is also doubted because of the reality. Detailed analysis to the root of workflow's problem is given in this paper. With the trend of network service, the future target of workflow is described. At the same time, the expression form for workflow accordant to its target is presented, which is based on event mechanism. At last, the necessity of the renovation to the architecture of workflow is dissertated.

Keywords: Workflow, Network Service, WFMS (Workflow Management System), Procedure Service, Event Mapping.

1. INTRODUCTION

The term of workflow came forth about 20 years ago. Comprehensive and deep researches have been done in this field by institutes and enterprises all over the world [1]-[6]. In 1995, WFMC (Workflow Management Coalition) constituted the standard for workflow [7], which indicated that the development of it began to be regular. The conception of workflow is accepted by more and more people. Today, a variety of workflow products can be acquired and its production value has become considerable.

However, another phenomenon also should be paid attention to when great progress is made in workflow. There still exists quite a big gap between people's expectation for it and its present status. Furthermore, it seems that the gap can't shrink under the architecture from WFMC.

The core idea of workflow is to separate procedure management from professional operation. But it's found that many procedure problems are coupling with professional operations in reality. In order to solve the coupling problem, lots of flexible methods are presented, and a new term of flexible workflow was brought out. Yet all the methods of flexible workflow are application oriented. As result, the procedure becomes unified with the profession again. It leads to doubts to the idea of workflow: can procedure management really be separated from professional operation? It's certainly quite a serious question. This paper will try explaining the question with detailed analysis of the development of the network service, the demand of flow task and the architecture of WFMS.

2. NETWORK SERVICE AND MIDWARE SYSTEM

Since workflow is a kind of advanced network service, it's better to begin with the discussion about the network. So the function of workflow can be understood more explicitly.

The appearance of network made computers linked together. Only the function of basic communication is provided in the network primitively. Then, combined with programming technique, RPC (Remote Procedure Call) is produced, which is based on the simple communication. Then, with the popularity of OO (Object Oriented) method, RPC is wrapped with object form, which is called distributed object. Distributed object has different name in different systems, for example, DCOM in Windows, CORBA in OMG and RMI in Java. RPC and distributed object are the expansion of basic communication. Customarily, distributed object is called network service. It's in higher layer of the network.

In traditional distributed object system, the client (the user of the service) and the server (the provider of the service) are bound together. It means that a DCOM client can't access a Java server. Obviously, people hope no such restriction, especially in Internet. An open protocol solved the problem. It allows the service spanning different systems. This protocol is called WEB Service, which came into being at the beginning of 21st century.

It's a big progress from basic communication to WEB Service. Yet the structure of the service varies little. They may all be regarded as a dot-to-dot structure, one is the client and the other is the server. Although there're usually many servers to provide the service physically, whole servers are unitary for the client logically.

The development of network service gave tremendous impact to software system. A new layer called midware system has appeared, the main function of which is to support network service. Corresponding to the sort of distributed object, there're all kinds of midware systems such as COM, .NET, Obix and WEB Logic. Midware system may produce the proxy for network service automatically. So the client can't distinguish whether the service is remote or local and also it needn't care for it. At the same time, the design and the implementation of network service are maintained consistent with those of local service as soon as possible with the support of midware system. For example, it's only needed to announce "WEB Method" for a method used as WEB Service in .NET platform.

Summarily, it can be said that network service has covered local service formally with midware system. Local service becomes a particular form of network service, where the client and the server are in one physical node. The network is made fully transparent to the client.

3. FLOW、PROCEDURE AND WFMS

Most of present software systems are of dot-to-dot structure. Now, the question is whether this structure is enough for us. If the task is relatively little, the answer is yes. Yet if the task is big, dot-to-dot structure won't be fit for it well. What are big tasks? Consider the examination and the approval of documents, comprehensive financial affairs and the management of product line, etc. Their common characteristic is of flow. The collaboration in some sequence is required there with a group of dots, actually a group of clients. Such kind of task is called flow task. It can be seen that the demand of flow task is beyond the capacity of dot-to-dot structure. There're two modes to deal with it:

(1) Dot-to-dot structure plus manual procedure management. Every step of a flow task can be regarded as a network service. When a step is over, manual form may be used to control the procedure, such as phoning, Email and the delivery of documents. Manual form is able to get maximal flexibility. Nevertheless, the disadvantage is also evident. First, the efficiency is very low. Second, it isn't reliable because it depends on people's understanding of the flow entirety. Mistakes will be made inevitably when the logics of the flow are complex.

(2) Flow software which processes the ability of automatic procedure management. Manual form is based on such fact as people know the information of the flow, for example, the executor of the next step, phone number and Email address. All the information can be saved in the computer, so the computer can manage the procedure too, even can do better. The fundamental of flow software is to create a status space which is corresponding to the executing process of the flow. It maintains and updates the status automatically. With the information of the status, the software assigns the task of the next step to proper executor when one step is fulfilled.

Flow software upgrades network service to a higher rank. That's the automatization of procedure management, which expands the scale of network service. Not only a pair of dots can be supported, but also a group of dots can now.

Flow software disposes of the procedure as well as the profession. So there're two sorts of logics in the flow software: procedure logic and profession logic. Profession logic is in every step and procedure logic is in the transfer between steps. They're independent on each other to a great extent. Supposing that a flow task can be regarded as a flow graph[8]-[10], procedure logic is the structure of the graph and profession logic is the property of the node. Thereby, procedure management may be separated from profession operation. That's the idea of workflow. With the idea, a kind of software is developed for general procedure management. It's called WFMS.

Such idea emerged in 1980s. WFMC regulated the related conceptions and terms afterward. Theoretically, it seems that WFMS make it easy to implement flow software. Linked with modules for profession operation, WFMS will become flow software for any specific profession. However, the practice isn't so optimized.

4. THE DEFECT OF FLOW GRAPH AND WFMC'S ARCHITECTURE

Today, when people talk about workflow, they have to face such a phenomenon that most of flow tasks don't depend on WFMS but on specific flow software or even manual form. Some people ascribe it to the custom and the fogyism. But it isn't so simple certainly. Why don't people adopt new technology if they benefit much from it? So, that's more the selection after the comparison between old working form and new one.

It's known that the prominent merit of manual form is the flexibility. Computer can't compete with people there. Fortunately, most work is relatively regular so that the predominance of the computer is able to exert. But it doesn't mean that the flexibility is inessential. On the contrary, it's very important for the software.

The criterion about the flexibility of the software is reusing ability. It often determines how much manual work can be replaced by the computer. The superficial meaning of the reusing is to use software modules repeatedly. Yet the exact meaning is to rebuild new software rapidly. Concretely for workflow, the reusing is to reconstruct flow software when professional demand varies.

It seems that researches of workflow have neglected the importance of the reconstruction. The reflection is that workflow is regarded as flow graph all along. Let's show the defect of flow graph with a simple example.

Supposing there's a loan task as Fig.1. The manager is charged for the examination if the loan value is higher than 100 million. Otherwise, the staffer is charged. Later, the rule varied. The threshold is improved to 200 million.

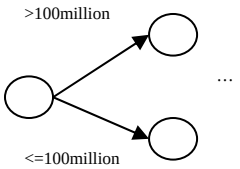


Fig.1. A part of loan task

Obviously, flow software for the profession need to be reconstructed to cope with the variety. What we most care for is whether it's easy to reconstruct it under present architecture of WFMS.

The present architecture of WFMS[11] is shown in Fig.2, which is based on the theory of flow graph and WFMC's referenced model. Workflow engine is the core of the architecture, which is charged for procedure management. The foundation of the management is the procedure definition, actually is the definition of flow graph.

The loan value is a professional data. But unlike other professional data, it's also related with the procedure. In the architecture of Fig.2, that data is put into the place called "relative data", which is generated by the application and used by workflow engine. Thus it can be seen that workflow engine is coupling with the profession in fact. If the loan threshold varies, workflow engine certainly has to be modified. In the application, relative data may often varies, not only the value but also the form. For example, the loan rule can varies as follows: who is charged for the examination depends on both the loan value and loaner's credit.

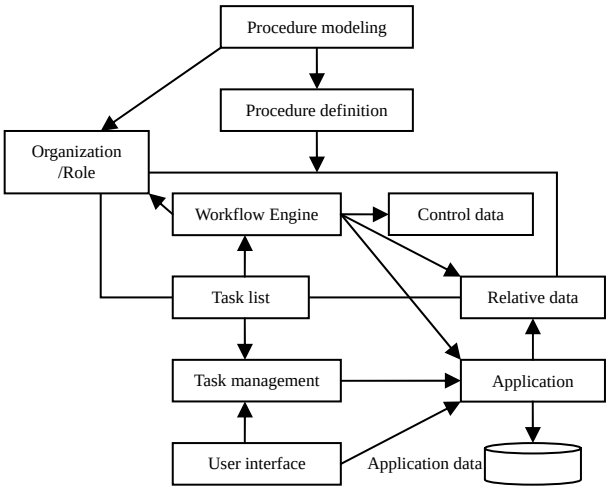


Fig.2. The present architecture of WFMS

Since almost all workflow products have used this architecture, none of them can deal with the variety easily. The problem produced tremendous negative infection to workflow. It's hoped that workflow is able to separate procedure logic from profession logic. But the fact is that the reconstruction of the flow is still difficult. Some people argue that workflow is only suitable for the instance that the professional data isn't related to the procedure entirely, which is evidently unconvincing.

In order to reducing the price for the reconstruction, additional specific module for relative data is added. WFMS with those modules is called flexible WFMS. Nevertheless, the varieties of relative data are so diverse and frequent that flexible modules also become a big burden. Furthermore, flexible modules are application oriented. Putting them into WFMS blurs the boundary between WFMS and specific flow software. So doubts about the rationality of workflow are understandable.

This paper deems that the problem lies not on the idea of workflow but on the theory of flow graph and the architecture of WFMC from that theory. The theory of flow graph has misdirected the development of workflow though it's easy to be accepted. Flow graph is the root of the problem.

5. PROCEDURE SERVICE ON EVENT MAPPING

The premise of solving the reconstructing problem is to grasp the essence of workflow exactly. It's necessary to discuss the question in the point of view of system service. It's known that network service for dot-to-dot structure is the system service today. Then, what's the one in the future? It should be the one that exceeds dot-to-dot structure naturally. That's procedure service which has been mentioned, namely workflow. So a new definition of workflow and that of WFMS are presented here:

Workflow is the general procedure service.
WFMS is the platform to provide procedure service.

The above definitions give expression to the essence of workflow more clearly compared with others. They abandon those subordinate factors.

The relation between workflow and network service is like that between network service and local service. Dot-to-dot structure is a particular form of workflow, where the task has only one step. WFMS makes the procedure transparent to the executors of flow task.

To realize the general service, a new expression form for workflow ought to be presented, which has more abilities than flow graph. Event form is adopted in this paper. Workflow can be regarded as a sequence of event mappings, which is shown as follows:

(1) $Action(condition(d^*)) \rightarrow Event$

(2) $\log ic(Event^*) \xrightarrow{f} (Role^*, Operation)^*$
$Operation : (\Pr ogram, Data)^*$

(3) $Workflow : (Event^*, Role, Operation)^*$

In the above, action is a part of operation, which is related to the procedure. d denotes professional data which affects the procedure. Condition denotes the formula about d; * denotes multiple. Role denotes the executor. Operation denotes profession disposal. Logic denotes the combining form of multi-events. f denotes the mapping form.

Event is abstract. An action can cause an event and the happening of the event can cause the reasoning on the rules of event mappings. The result of the reasoning indicates the operation on some role in the next step. There're three forms for event mapping:

(1) Fixed mapping. It means that the flow will transfer to a fixed role when a step is over. Flow graph is of this kind.
(2) Finite mapping. It means that the flow will transfer to some roles in a finite group. For example, the manager and staffer in loan profession is a finite group.
(3) Random mapping. It means that the flow will transfer to any role which entirely depends on the professional data. In this circumstance, no flow graph can be drafted.

Those three mapping forms cover whole demands of procedure service. For flow tasks, the expressing ability of event mechanism exceeds that of flow graph much more.

Also, event mechanism is far better for the reusing of the flow. The action is isolated to the procedure by the event. Both the relation of action to event and that of events to role can be varied with the form of the definition. So it can be adapted to the variety of the profession well.

Expressing the flow task in Fig.1 with event mechanism is shown as follows:

$Action =$ the submission of loan form

$d =$ loan value

$Action(value \le 100million) \rightarrow e1$

$Action(value > 100million) \rightarrow e2$

$e1 \rightarrow (Staff, Audit)$

$e2 \rightarrow (Manager, Audit)$

When the profession varies, for example, the expressing form can be varied as follows:

$d =$ loan value, credit degree

$Action(value \le 200million, credit = low) \rightarrow e1$

$Action(value > 200million, credit = low) \rightarrow e2$

$Action(credit = high) \rightarrow e3$

$e1 \rightarrow (Staff, Audit)$

$e2 \rightarrow (Manager, Audit)$

$e3 \rightarrow (Staff, Audit)$

It can be seen that event mechanism possesses an excellent structure. Deferent parts of it are quite independent and modifications can be made by the definition. So, It's a good choice to express workflow with the form of event mapping.

In WFMC's referenced model, there's no consideration for the event, only for flow graph. To establish the architecture for general procedure service, it's necessary to renovate present architecture of WFMS. The conceit of the renovation is shown in Fig.3. Unclear "relative data" doesn't exist any longer. A new module called event processing is added in. It's in the middle of the application and workflow engine. The module of event processing possesses a general structure just like that in GUI system.

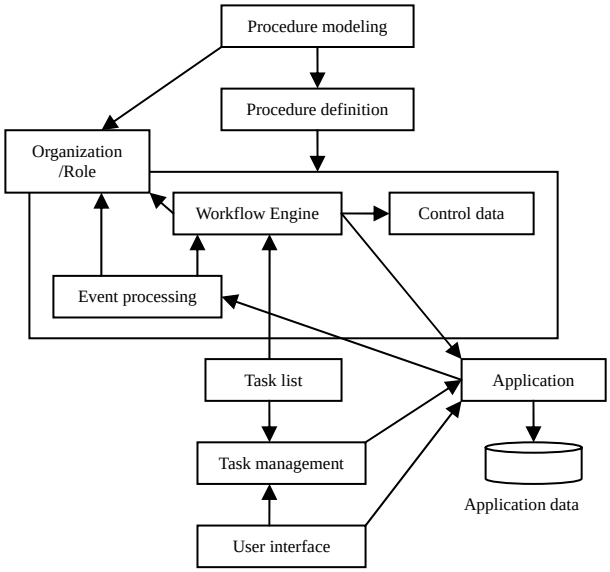


Fig.3. The renovation to the architecture of WFMS

6. CONCLUSIONS

The idea of workflow is significant. The development of it doesn't go very well just because it's plunged into flow graph so deeply.

In the view of the system service, flow graph is unnecessary. The essence of workflow is procedure service which ought to be independent on the application. The renovation to the architecture of WFMS will give huge impact to whole software system. WFMS may be the platform of future network service though a lot of efforts need be paid.

REFERENCES

[1] Kacmar C, Carey J, Alexaander M, "Providing workflow services using aprogrammable hypermedia environment", *Information and Software Technology*, Vol.40, No.7, 1998, pp.381~396.

[2] Papazoglou M, Delis A, Bouguettaya A et al, "Class library support for workflow environments and applications," *IEEE Transactions on Computers*, Vol.46, No.6, 1997, pp.673~686.

[3] Vander Aalst W M P, "Three good reasons for using a Petri-net-based workflow management system," In: Navathe S, in *Proceedings of the International Working Conference on Information and Process Integration in Enterprises*, Camebridge, MA: Kluwer Academic Pub., 1996, pp.179~201.

[4] Marshall C, "Enterprise modeling with UML: designing successful software through business analysis," Addison-Wesley, Reading, MA, 2000.

[5] Lee H, "A workflow-based methodology for developing hypermedia systems," *Journal of Organizational Computing and Electronic Commerce*, Vol.11, No.2, 2001, pp.77~106.

[6] Kappel G, Lang P, "Workflow management based on objects, rules, and roles," *IEEE Bull. Technical Committee Data Eng*, Vol.18, No.1, 1995, pp.11~18.

[7] Workflow Management Coalition, "The workflow reference model," *Technical Report, WFMC-TC00-1003*, Hampshire: Workflow Management Coalition, 1995.

[8] Salimifard K, Wright M, "Petri-Net-based modeling of workflow systems: an overview," *Eur. J. Oper. Res*, Vol.134, No.3, 2001, pp.664~676.

[9] Weitz W, "Combining structured documents with high level Petri-Nets for workflow modeling in internet-based commerce," *Int. J. Cooperative Inf. Systems*, Vol.7, No.4, 1998, pp.275~296.

[10] Sadiq W. Sadiq M, "Analyzing process models using graph reduction techniques", *Inf. Systems*, Vol.25, No.2, 2000, pp.117~134.

[11] Jablonski S, Bussler C, "Workflow management: modeling concepts, architecture, and implementation," International Thomson Computer Press, London, 1996.

Xin Li is a Full Professor in Department of Computer Science, Shantou University. He graduated from Northwestern Polytechnic University in 1997 with bachelor's degree of specialty of computer application; from Northwestern Polytechnic University in 1999 with master's degree of specialty of computer application; from Northwestern Polytechnic University in 2002 with Phd's degree of specialty of computer software and theory. He was a lecturer in Department of Computer Science, Xiamen University (2002~2006); was a postdoctoral fellow, postdoctoral workstation in Xiamen Longtop System Co. which is allied with the Institute of Computer in National University of Defense Technology (2003~2005). He has published about 20 papers. His research interests are in distributed computing, workflow, and midware system.

Fuzzy Reliability of Mirrored Storage System Based on iSCSI*

Minghua Jiang[1], Jingli Zhou[2], Ming Hu[3]
[1]College of Computer Science &Technology, Wuhan University of Science &Engineering
Wuhan, Hubei 430073, China
[2]Key Laboratory of Data Storage System (Huazhong University of Science &Technology), Ministry of Education
Wuhan,Hubei 430074, China
[1]Email: jmh@wuse.edu.cn

ABSTRACT

iSCSI is a newly emerging protocol with the goal of implementing the storage area network (SAN) technology over TCP/IP, which brings economy and convenience whereas it also raises performance and reliability issues. This paper presents three implementations of mirrored storage system based on iSCSI, then the membership function of the states is defined and the reliability of mirrored disk system is analyzed by using the reliability theory based on fuzzy state.

Keywords: iSCSI, Mirrored Storage System, Fuzzy Reliability, Fuzzy Logic

1. INTRODUCTION

Storage systems represent a growing market due to the enormous volumes of data generated and used by today's application. To meet these storage demands, there have been many recent developments in the storage market. These include Network Attached Storage (NAS) and Storage Area Network (SAN) which allow clients to by-pass the server and access storage devices directly. Mirrored storage system has become increasingly important as enterprises and businesses depend more and more on data. It has been widely deployed in financial enterprises and other businesses for tolerating failures and disaster recovery. Traditionally, such remote mirroring is done through dedicated SAN (storage area network) with FC (Fiber Channel) connections that are usually very costly in terms of installation and maintenance, RAID (Redundant Array of Independent Disks) is a known, mature technique to improve performance and reliability of disk I/O through parallelism and redundancy. Internet small computer systems interface (iSCSI) is emerging as an end-to-end protocol for transporting storage I/O block data over IP networks [1]. As a low cost alternative to the FC protocol for remote storage, iSCSI greatly facilitates remote storage, remote backup, and data fault tolerance. Therefore, the iSCSI lends itself naturally to a cost-effective candidate for Mirrored storage system making use of the available Internet infrastructure.

Mirrored storage system, which corresponds to RAID1 is the focus of this paper. RAID1 replicates data on two disks to attain fault-tolerance, i.e., if one of two disks fails, data is accessible from the other disk. In basic mirroring data is written onto N/2 primary disks, which are then mirrored on N/2 Secondary disks. This RAID1 organization can obviously tolerate up to N/2 disk failures, as long as all failed disks are either all primary or all secondary disks. On the other hand the failure of a disk results in halving the maximum disk access rate is processing read requests for that data. Fuzzy reliability theory in its various forms found applications, especially in fault tree analysis, reliability optimization and risk analysis. However, fuzzy mathematical techniques can be successfully applied to conventional reliability theory, without taking recourse to any form of the fuzzy reliability theories. In this paper we investigate the fuzzy reliability of several RAID1 organizations proposed to alleviate the shortcomings of the basic RAID1 organization. Reliability is specified as the probability that there is no data loss.

In this paper we review two disk organizations, which have been proposed to attain more balanced disk loads than basic mirroring upon disk failure. This is achieved by distributing the data and the associated read load of a failed disk across multiple disks.

2. RELIABILITY THEORY BASED ON FUZZY STATE

Fuzzy set theory has been applied to reliability theory /engineering with great success in the past two decades. The incorporation of the fuzzy set theoretic concepts into the multidisciplinary area of reliability theory has been done by modifying the basic assumptions underlying the definition of reliability of a component or system. Conventional reliability theory is based on, among others, the following two fundamental assumptions [2].
(1) Binary state assumption: the system can only be in either of the two crisp states viz. fully functioning or fully failed.
(2) Probability assumption: the system failure behavior is fully characterized by the probability measures.

Although, these two assumptions are often valid, they are not reasonable in a large variety of cases. This called for the incorporation of the concepts of fuzzy set theory into these assumptions.

Thus, 1) and 2) are modified as follows [2].
(1') Fuzzy state assumption: the system success and failure are characterized by fuzzy states. At any given time the system can be viewed as being in one of the two states to some extent. Thus, system failure is not defined in a binary way, but in a fuzzy way.
(2') Possibility assumption: the system failure behavior is fully characterized by the possibility measures.

For the sake of simplicity, the conventional reliability theory is called "PROBIST reliability theory," since it is based on assumptions 1) and 2). When 1) is replaced by 1') and 2) is replaced by 2'), the resultant is called fuzzy reliability theory.

Thus fuzzy reliability theory manifests itself in three different forms viz. PROFUST reliability theory, POSBIST reliability theory, and POSFUST reliability theory [2].

* This work is Supported by Scientific Research Fund of Hubei Provincial Education (No: 2004D009) and Hubei Provincial Natural Science Foundation of China (No: 2004ABA015).

Assuming that the mirrored disk arrays system have non fuzzy states $S_0, S_1, \ldots, S_n$, U={ $S_0, S_1, \ldots, S_n$ } is domain. S: S={$S_i,\mu_S(S_i)$ i=0,1,…,n} is defined as fuzzy success state and F: F={$S_i,\mu_F(S_i)$ i=0,1,…,n} is defined as fuzzy failure state. $\mu_S(S_i)$ and $\mu_F(S_i)$ are relative membership function.
The transition from S_i to S_j is denoted as m_{ij}, and

$$T_{SF}=\{(m_{ij}, \mu_{T_{SF}}(m_{ij}) \quad i,j=0,1,\ldots, n), \tag{1}$$

Membership function is defined as the following formula:

$$\mu_{T_{SF}}(m_{ij}) = \begin{cases} \beta_{F/S}-\beta_{S/F} & \beta_{F/S}>\beta_{S/F} \\ 0 & \beta_{F/S} \le \beta_{S/F} \end{cases} \tag{2}$$

$$\beta_{F/S}=\mu_S(S_i)/(\mu_S(S_i)+\mu_S(S_i)) \tag{3}$$

T_{SF} is transfer from fuzzy success state to fuzzy failure, and as a fuzzy event. So, fuzzy reliability is denoted as:
$R(t_0, t_0+t) = P\{ T_{SF}$ cannot happened in $[t_0, t_0+t]\}$

$$=1-\sum_{i=0}^{n}\sum_{j=0}^{n}\mu_{T_{SF}}(m_{ij})P\{m_{ij} \text{ can happened in } [t_0, t_0+t]\}$$

$$=1-\sum_{i=0}^{n}\mu_{T_{SF}}(S_i)\,P\{\text{the system is in } S_i \text{ state at } t_0+t\} \tag{4}$$

In which case R (0, 0+t) =R (t).
The equation (4) expresses the fuzzy reliability of the system at the t moment. It can be interpreted as the probability that the system can damage with certain degree between (0, t).

In Mirrored disk arrays system, the reliability of a disk is the probability that if a disk functioning at t=0, it will be still functioning at time t. The analysis of data related to disk failures shows that the reliability of a single disk can be approximated by an exponential distribution: $R_{disk} = e^{-\lambda t}$, $t \ge 0$.

Assuming that disk have a constant failure rate,
P(the system is in S_k at t) =A(k)R_k(t) (5)
A(k) is the number of case that system can tolerate k disk failures, so A(0)=1 and A(k)=0, k>M, since at best the failure of M disks can be tolerated. $R_k(t)$ is the probability that in a certain system configuration k disks are functioning and N-k disks have failed:

$$R_k(t)=R_{disk}^k(t)(1-R_{disk}^k(t))^{N-k}=e^{-k\lambda t}(1-e^{-\lambda t})^{N-k} \tag{6}$$

From (4)-(6), the fuzzy reliability R(t) for N=2M disk is given as follows:

$$R(t) = 1-\sum_{k=0}^{M}\mu_{T_{SF}}(S_k)A(k)R_k(t) \tag{7}$$

3. ARCHITECTURE AND MIRRORED DATA ORGANIZATIONS

3.1 Architecture

The mirrored storage system based on iSCSI in this paper is composed of primary iSCSI target node and secondary iSCSI target node. Each iSCSI Target node comprised a set magnetic disk drives as illustrated Fig.1 and is directly connected to LAN network or WAN network. Several server hosts are connected to a fault tolerant storage system through a Cisco 3550-12T Gigabit Ethernet switch. The server hosts act as iSCSI as an iSCSI initiators while the mirrored storage nodes acts as an iSCSI target. The iSCSI initiators in the LAN inside ore laboratory are connected through our campus network and leased lines to the educational Internet.

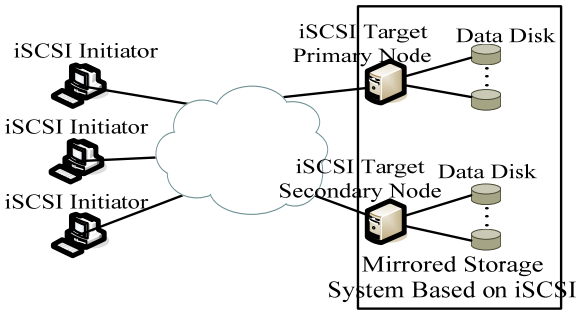


Fig.1. Mirrored Storage System Based on iSCSI Architecture.

Failing or failed the system is prevented from delivering services and accessing data. Failed software components can be restarted within the system, and failed iSCSI target nodes may return to the system following repair. Mirrored storage system is to organize the iSCSI targets similar to RAID by using mirroring techniques, each iSCSI target is a basic storage unit in the system, and it server as storage device node. All the nodes in the array are connected to each other through a high-speed switch to form a local area network. Data are divided into many blocks and the blocks are distributed among all disks and iSCSI target nodes. All iSCSI target nodes are identical, each node containing the same number of disks M. The total number of storage system disks N is then N=2*M.

3.2 Mirrored Storage System Based on Organizations

Three mirrored disk organizations are described in this paper: (1) basic mirroring (BM), (2) interleaved declustering (ID), (3) chained declustering (CD), and then these methods are compared qualitatively from the viewpoint of load balancing and obtain A(k) in each case.

3.2.1 Basic Mirroring

Basic mirroring is the most common type mirroring and there are N=2M disks with disk 2i mirroring disk 2i-1, $1 \le i \le M$, and vice-versa. The basic RAID1 organization can tolerate up to M disk failures, as long as the failures are in different mirrored pairs. However, data loss is possible even with two disk failures when they constitute a pair. There are M=N/2 ways for the second mirrored disk failure to lead to data loss, while there C_2^N ways for two disk failures. The probability of data loss due to a second disk failure is then 1/(N-1). Fig. 2 shows a basic mirroring organization with striping. The number of ways that k disk failures don not lead to data loss equals the number of ways of having a single failed disk per pair [3].

$$A(k) = C_k^M 2^k, 1 \le k \le N/2. \tag{8}$$

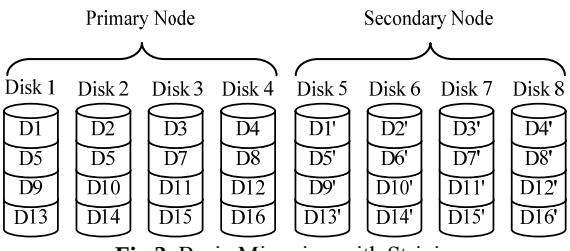


Fig.2. Basic Mirroring with Striping

3.2.2 Interleaved Declustering

In [4] interleaved declustering is considered as a replication scheme at the logical level. It can also provide an alternative to

the mirroring scheme, if applied at the physical level. We briefly describe this scheme, which is illustrated in Fig.3, as applied to physical level replication. The Secondary storage subsystem is divided into disk clusters, each of Size M, e.g., in Fig. 2, M=4. The primary data resides on each one of disks in the cluster, and the backup data is divided equally among the remaining M -1 disks of the cluster. During normal operation, read requests are directed to the primary data and write requests are directed to both copies. When a failure occurs, the read workload that was destined for disk 1 can be distributed among the surviving M -1 disks of the cluster in which the failure occurred. This is an improvement over the mirrored disks scheme where the additional workload, which was destined for the failed disk, ends up on a single surviving disk

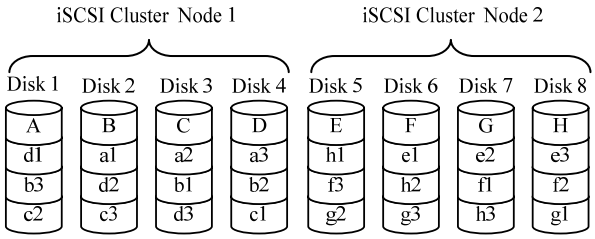


Fig.3. Interleaved Declustering

Given that there are clusters, then the number of disks per cluster is M=N/c. After the first disk failure, the probability that a second disk fails in the same cluster equals the ratio of the number of surviving disks in the cluster and in the system:(M-1)/(N-1). When $k \le c$ disks fail, data loss will not occur if all the fail disks are in different clusters, so that:

$$A(k) = C_c^k M^k, 1 \le k \le c, M = N/c. \quad (9)$$

3.2.3. Chained Declustering

In [3][5], chained declustering is considered as a replication scheme at the logical level of a shared nothing database machine. This scheme can also provide an alternative to the classical mirroring scheme when applied to physical level replication, as well as to the interleaved declustering scheme described in [4], We briefly describe the concept of chained declustering from [5].

Chained declustering has the same storage overhead as compared to the classic mirroring scheme and interleaved declustering, but it was proposed in [5] to attain a higher reliability level than interleaved declustering. Chained declustering can also lead to a more balanced load than interleaved declustering in processing read requests. With a single disk failure the read load of surviving disks increases to M/(M-1) of the original load, rather than M/(M-1) with M=N/c in chained declustering.

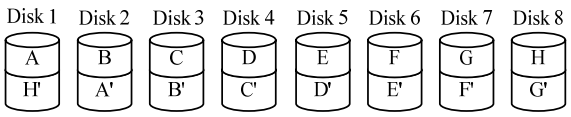


Fig.4. Chained Declustering

It can be seen from Fig. 4 that it takes the failure of two consecutive disks for data loss to occur. The number of cases resulting in data loss with i=2 disk failures is N. It follows:

$$A(2) = C_N^2 - N = \frac{N(N-3)}{2} \quad (10)$$

In general [3],

$$A(k) = C_{N-k-1}^{k-1} + C_{N-k}^{k}, 1 \le k \le M \quad (11)$$

4. NUMBERICAL RESULTS

In this section, the fuzzy reliability analysis of mirrored disk organizations is described. We assume that mirrored disk system is composed of 32 disks, in Interleaved Declustering mode, the parameter c is 8. The mean time to failure of a disk driver (1/λ) is 20000 hours.

The membership function for the states using in this numerical analysis is quadratic.

$$\mu_{T_{sp}} = \begin{cases} 1 - \frac{2i^2}{M^2}, 0 \le i \le M \\ \frac{2(M-i)^2}{M^2}, \frac{M}{2} < i \le M \end{cases}$$

The parameter to consider is the time step t, the fuzzy reliability will be estimate each 10 hours (t=100) for 87600 hours (10 years). The result from formula (7) is presented on Fig 5.

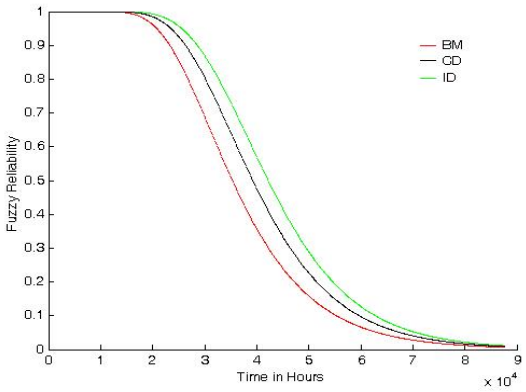


Fig.5. Fuzzy Reliability of Four Mirrored Disk Organizations

5. CONCLUSIONS

Reliability models for various fault tolerant storage system architectures are developed. Fuzzy logic is very useful calculating with fuzzy state. The paper has described three mirrored storage organizations and in each case, obtained a closed form expression for A(k) where k disk failures are tolerated in the system of N disks. As a result, this analysis provides reliability curves that show the variation of the "fuzziness" degree of reliability at each instant of time. With the traditional approach, based on crisp values, getting the intervals of the reliability would require a separate model run and would result in family of curves open to interpretation.

REFERENCES

[1] S. Aiken, D. Grunwald, A. Pleszkun, and J.Willeke, "A Performance Analysis of the iSCSI Protocol," *20th IEEE Conference on Mass storage Systems and Technologies*, 2003, pp.123~134.

[2] K.Y.Cai, C.Y.Wen, M.L.Zhang, Fuzzy Variables as a Basis for a Theory of Fuzzy Reliability in the Possibility Context, Fuzzy Sets and Systems, Vol.42, 1991, pp145-172.

[3] A. Alexander Thomasian, M.Blaum, "Mirrored Disk Organization Reliability Analysis," *IEEE Trans. Computers*, Vol. 55 No.12, December 2006, pp1640~1644.

[4] G.Copeland, T.Keller, "A Comparison of High-Availability Media Recovery Techniques", *SIGMOD Conference*, June 1989, pp 98~109.

[5] Hui-I Hsiao , David J. DeWitt, "Chained Declustering: A New Availability Strategy for Multiprocessor Database Machines", *Proceedings of the Sixth International Conference on Data Engineering*, February 1990, pp.456~46.

Web Proxy Caching Scheme Based on Multilist Structure Mixed Policies*

Mingwu Zhang, Bo Yang, Shenglin Zhu
College of Software Technology, South China Agricultural University
Guangzhou, Guangdong 510642, China
Key Lab of Guangdong Electronic Commerce Market Application Technology
Guangzhou, Guangdong 510320, China
Email: scauzhang@gmail.com

ABSTRACT

The Web is growing rapidly and revolutionizing the means of information access. Web caches are different from processor caches because web caches have several additional criteria, such as frequency and recentness of pages, size of a document, cost of fetching a document etc. It has been shown that, the classical LRU replacement policy performs poorly in Web caches because the above criteria decrease hit rate and increase eviction latency and access latency of Web request. In this paper, in order to improve proxy's speed and hit rate, a three-class-list structure is used to organize the index of html elements in cache. It gives a lifetime-cycle algorithm and out-of-date replacing policies for web cache replacement, which based on a mixed policies including LFU, LRU, long term static element factor and network bandwidth factor. Experimental results show that three-class-listing structure to perform the mixed replacement policies and out-of-date factors, the pages hit rates arrive at 50% when cache size is about 500M, which has a fast step compared by 3.7% in traditional LRU-based ones.

Keywords: Cache Scheme ,Web Proxy, Replacement Policy

1. INTRODUCTION

The rapid increase in web usage has led to dramatically increased loads on the network infrastructure and on individual web servers. Web proxy plays a key role in improving the efficiency of accessing Web pages[1-3]. Caching at proxy servers is one of the ways to reduce the response time perceived by World Wide Web users. Either by configuring mirror of Web pages or by setting cache in user's computer directly, it conducts cache to the pages which are accessed frequently, so as to improve the access efficiency of the network. It has been shown that, the classical LRU replacement policy performs poorly in Web caches because it decreases hit rate and increase eviction latency and access latency of Web request[7-9].

Maximum caching efficiency is achieved when content is successfully distributed to the end user. Caches must cooperate such that only one copy of the file is ever downloaded into a given local system. High ache hit rates are a unction of cache size which in turn is a function of the number of users connected to that cache. Files should only be purged when they are known to be obsolete rather than rely on predictive methods. If this is done properly, it will be possible to operate caches which are many times the size of current caches and which are guaranteed to contain only the current information.

* This work is partial supported by the National Natural Science Foundation of China for contract 60573043, and the Foundation of National Laboratory for Modern Communications under Grant 9140c1108010606, and Foundation of Key Lab of Guangdong Electronic Commerce Market Application Technology

When a request is launched for a Webpage by a user, it is sent to the proxy server. If the page misses in the cache, the proxy will direct the request to appropriate remote information server. The source files of the internet pages which were accessed recently are saved in Web proxy, and whenever these files are to be requested the next time, according to their given period value, the files will be decided whether to fetch in the local cache or to fetch the new files from remote server.

Consequently, the documents that took a long time to fetch are preferentially kept in the cache, and documents that are infrequently updated and thus seldom require validations are preferentially stayed in the cache.

Through analyzing the implementation procedure of method of cache of the web proxy, a page cache scheme, to organize and search cache content based on three-class-listing index is put forward in this paper, and it gives the cache replacement scheme composed by mixed of LFU, LRU, and long term static consideration etc. In this paper, we analyze and discuss the ways to improve pages' hit rate, lifetime-cycle, frequency of access，and out-of-date superseding of cached web pages based related algorithms.

2. RELATED WORKS

In [3], Papadimitriou et.al presented a model of Web communities which constituted a part of the Web structure. The proposed model is aimed at characterization of the topology behind the Web communities. It is inspired by small world graphs that show behaviors similar to many natural networks. Edmond et.al [8] suggested that the Website be modeled as a directed graph in which a node represents a Web page and an edge represents a hyperlink. It is essential for designing efficient algorithms for crawling, searching, and ranking Web resources.

Vakali[9] presented an extension to the conventional LRU algorithm by considering the number of references to Web objects as a critical parameter for the cache content replacement. The proposed algorithms are validated and experimented under Web cache traces provided by a major Squid proxy cache server installation environment. But author improved algorithm considers the LRU and HLRU based history based approach to the Web proxy replacement process that is impact and effectiveness on the Web cache content replacement.

Hao et.al[4] presented an approach to successfully predict Web pages that are most likely to be re-accessed in a given period of time using neural network model. It used an intelligent predictor that can be implemented on a Web server to guide caching strategies, which based on a back-propagation learning rule. It adapted to long-range prediction accuracy in static Web site structure. Jose et.al [10] introduced a ranking based on the frequencies of user clicks on the outer-links in a page that are

captured by navigation sessions of users through the web site. It implied that the topology of a web site is very instrumental in guiding users through the site. So, we will improve Webpage hit rate when a request launched, an effective page returned.

We introduce a multi-list policy to describe Website and Webpage structure, and also propose a lifetime-cycle algorithm and out-of-date replacement policies so as to improve hit rate.

3. WEB PROXY

3.1 Proxy Procedure

The context of a Web page is made up of elements such as texts, pictures, sounds, forms, hyperlinks and so on. In such a page, these elements are saved in web server as independent files. When client needs to display a web page, it lists all the elements contained in the page. Every procedure of getting a file is called a http transaction. There are a series of http transactions in listing a complete web page and these transactions are non-status between them. The procedure of a http transaction consist of 4 steps:

STEP 1: A first, building up a http link. When client asks server for a web element, a TCP of http transaction must be built up. A link can only perform a http transaction.

STEP 2: Send a request to proxy server and proxy resend message to Web server. Every request that client makes begins with method command and follows with a URI(Uniform Resource Indicator) which is a string to determine a certain object address on the web. Some information that client provides for the server itself should also be added after the URI by client, such as http protocol version, request header type and so on. Usually there are mainly three types of requesting method: *put, get* and *post*. *Put* model is used to delivery the data information to server; *Get* model is to extract file or state information from server; and *post* mainly to submit form information to server so as to implement the bio-direct data exchange between client and server.

STEP 3: Server responds the request. After the server received the client's request, it makes appropriate respond according to the request method and type. Respond information begins with http version, and follows with respond reason and code information, so as to answer client's request.

STEP 4: Disconnect the link. After server responds customer's request, it should cut down the link with client so as to accept other clients' request.

3.2 Proxy Cache

Web proxy accepts and analyses client's request, and then decides whether to fetch data in proxy cache or from remote information server, and then delivery it to client after fetching the data. Web proxy is like an transmitter. The aim of introducing web proxy lies in two factors: The first is to perform agency authentication. Web proxy gets the user's information so as to perform the authentication and permission management; the second propose is to improve access efficiency. The proxy delivery the data to client, it also saves it on cache itself. When others client wants to access the same page, it can get the data from local proxy server instead of remote server.

There are the new web sources in web proxy cache. According to that how to make the content in cache be new and excellent, proxy cache policy can be classified into *active cache* and *passive cache*. As for passive cache, the content can be renewed only when client makes request. While active cache is refreshed automatically while web content has been saved in cache before customer makes request for data.

Passive cache usually decides whether to get information in local cache or get the new data from remote web server by http protocol remark header, such as modifying time of source, http protocol header and so on. If there is not any change of web server's content, it will extract the data copy in cache to the client.

There are reserved way and automatic way in active cache. In reserved method module, administer needs to record some websites that need to perform cache policies and update cycle. While automatic method uses a certain algorithm to determine which data will be accessed again most possibly and it determines the cycle of prefetching data according to the access control policies.

4. CACHE SCHEME

4.1 Cache Scheme

BHA(Byte Hit Rate) and LH(Latency of Hit) are two important consideration to allocate cache size. BHA is a ratio that elements fetch in cache than to all. We denote the value of BHA by H, as

$$H = \frac{\sum_{i=1}^{n}(r_i - 1)}{\sum_{i=1}^{n} r_i} \quad (1)$$

Where r_i represent quotation frequent. Files i comes from files set $\{1, 2, ..., n\}$.

LH is a very important to considerate whether cache size is excellent. Page hit rate is about 24% if not any optimization approach[7]. In order to improve parameter value of PHA, it can expand cache capacity, but it will increment LH. We compose about LH and PHA when setting cache size. We denote the value of LH by C, as

$$C = \frac{\sum_{i=1}^{n} d_i(r_i - 1)}{\sum_{i=1}^{n} d_i r_i} \quad (2)$$

Where d_i is cycle time that between sending request and fetch data, and r_i represent quotation frequent.

4.2 Cache Index Structure

A http element is a unit object in cache, and we organize all cache content in three-class-list structure. We introduce list element as website element, html page element and page content element.

Website element, named *pWebpage*, is the root of cache content tree. *pWebpage* link saves all content about web page, for example, URL, IP, server name and other web information. We fetch the data from cache through IP ,URL or server name etc, and it can search out same result when perform the retrieval.

The element *pHtmlFile* is sublink of *pWebpage*, and it links several web page's element, for example, text, picture, sound etc. Furthremore, *pHtmlfile* pointer records the file's address and time information in the proxy cache.

The element pCacheFile, the leaf of the *pHtmlFile*, records http elements' infomation. It records http elements' filename, hit count, file length, last modified date, and so on. It is a key factor consideration for cache replacement.

When client gives a request for web, web proxy search *pWebpage* listas a list tree in local cache first. If it find out matched URL or IP in *pWebpage* link, it indicates that page hit is found and proxy server extract the data to client. Otherwise, it send the request to remote server for the new data. If *pWebpage can* match the request in cache pool, it will search *pHtmlfile* subtree for page's information about page's location and date, and then search the *pCacheFile tree* for page's validation. *pCacheFile* remarks some information about whether the page is out-of-dated, and the data that need deleted, or build up new link for new page elements. It can detect and notification service for web pages automatically.

4.3 Cache Replacement Algorithms

The number of references to web objects over a certain time period is a critical parameter for the cache content replacement. We consider for the simple consistency control and coherence policy.

It introduces an out-of-date factor, called ofd , to improve PHA. ofd is focus on the conditions:

(1) LFU(Least Freuency Used) factor *Ef*. LFU considers that used files are removed first. There is an attribute in pCacheFile list, and cache replacement algorithms search this tree periodically. It will not consider file size or download latency of the file and may keep obsolete files infinitely in the cache.

(2) LRU(Least Recently Used) factor *Er*. LRU associates with each file the time of that file's last be used. When a file be replaced, the file chosen is one that has not been used for longest period of time.

(3) Long term static element factor *Et*. In general, picture and sound files' replacement period is longer than text, furthermore, picture and sound files size is long than text. We can save picture and sound files in cache first.

(4) Network bandwidth factor Es. On the same condition, it should replace resource whose fetch time is short.

We use mixed factors to describe the replacement of cache. We give the policy of ratio parameter as

$$\text{Minmaxize } d = x_1 \times Ef + x_2 \times Er + x_3 \times Et + x_4 \times Es ,$$

$$\text{subject to } \sum_{i=1}^{4} x_i = 1 \qquad (3)$$

4.4 Experimental Results

Initial experimental to describe the pages hit rate for replacement factor *x*. In experiment, put and get method are tested because post method usually to operate database, it hasn't cached in proxy pool. We give four group of value for testing about factor in 100M cache size. Result shows that group 3 is better than others groups.

Table 1. Initial result for coeff factor

group no.	Ef coeff x_1	Er coeff x_2	Et coeff x_3	Es coeff x_4	ratio of page hit, S (%)
1	0.25	0.25	0.25	0.25	18.4
2	0.16	0.34	0.40	0.10	28.2
3	0.22	0.30	0.36	0.12	34.7
4	0.22	0.35	0.31	0.12	33.2

We give a comparison to LRU algorithm [9], which is based on the Temporal Locality Rule. In LRU, if the cache disk usage is closer to the low watermark(usually 90%) fewer cached Web objects are purged from cache, whereas the usage is closer to high watermark(about 95%) the cache replacement is more severe. We select coeff scheme about x_i with group 3 above

The performance metrics evaluation of web cache focus on the factors such as cache hit ratio and byte hit ratio, where cache hit ratio represents the percentage of all requests being serviced by a cache copy of the requested page that replacing the original objects, and byte hit ratio represents the percentage of all data transferred from cache, i.e. corresponds to ratio of the size of objects retrieved from the cache server. The valuation of cache hit ratio and byte hit ratio are considered to be the typical cache replacement policies.

The byte hit rate of our model and LRU-based algorithm are shown in Fig.1. Experimental result show that hit rate in our algorithm close to 50% when cache size is 500M bytes, where LRU-base model is 46.3%.

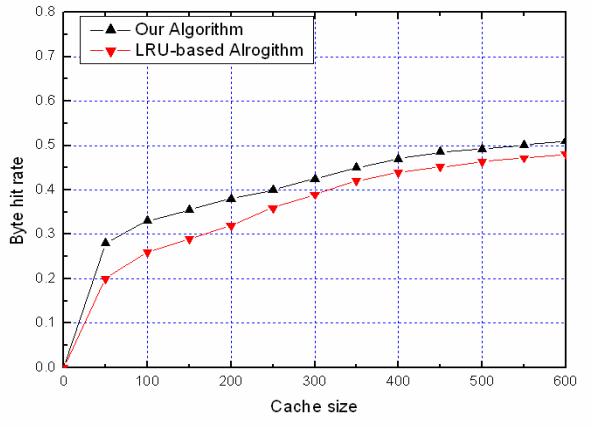


Fig.1. Byte hit rate by cache size

Fig2 depicts the bytes hit ratio for LRU-base algorithm and our algorithm model and with respect to the number of requests. Results show that when requester is small, the byte hit rate is low. With the increasing of requester, the byte hit rate increases.

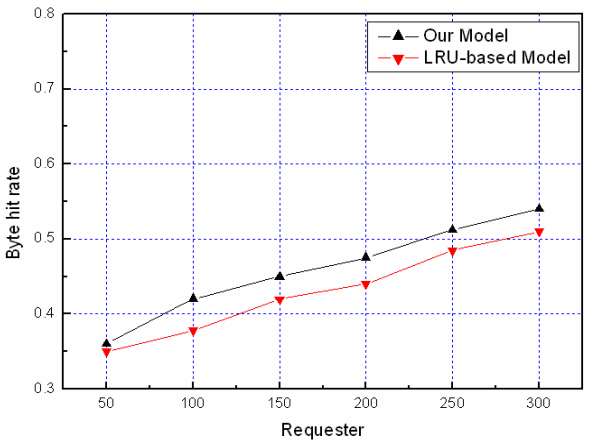


Fig.2. Byte hit rate by requester

5. CONCLUSIONS

We have proposed a multi-list structure Web cache structure model that describes Web page linking relationship.

Experiments show that our model with mixed replacement policies and out-of-date factors can improve the performance and pages hit rate, which is preceded to LRU-based model.
Web caching reduces network load, server load, and the latency of responses. By storing objects closer to the clients, web caches offer the benefits of reduced bandwidth usage, reduced server load, and lower retrieval latencies. To further improve client latencies, pre-fetching is often proposed in an attempt to retrieve objects in advance of a client request for further research.

REFERENCES

[1] Gyrgy Frivolt,and Moria Bielikov, *Topology Generation for Web Communities Modeling* .Lecture Notes in Computer Science, Volume 3381, 2005,167-177.

[2] Hou, Y.T, *On network bandwidth allocation policies and feedback control algorithms for packet networks.Computers Network*, 2006.32(3), pp.481-502.

[3] G. I. Papadimitriou , A. I. Vakali , G. Pallis , S. Petridou , A. S. Pomportsis, *Simulation in Web data management, Applied system simulation: methodologies and applications*, Kluwer Academic Publishers, Norwell, MA, 2006.

[4] Hao bo Yu,Lee Breslau,Scott Shenker, "An Adaptive Web Cache Access Predictor Using Neural Network" .Lecture Notes in *Computer Science*(Volume 2358),2002.

[5] Xueyan Tang , Samuel T. Chanson, "Adaptive hash routing for a cluster of client-side web proxies", *Journal of Parallel and Distributed Computing*, v.64 n.10,pp.1168-1184, Oct 2004.

[6] Dimitrios Katsaros , Yannis Manolopoulos, "Caching in Web memory hierarchies", *Proceedings of the 2004 ACM symposium on Applied computing*, Mar 14-17, 2004, Nicosia, Cyprus.

[7] Bhattacharjee, A. Debnath, B.K. "***A*** new Web cache replacement algorithm. Communications", *Computers and signal Processing*, 2005, pp.420- 423.

[8] Edmond H. Wu and Michael K. Ng. "A Graph-Based Optimization Algorithm for Website Topology Using Interesting Association Rules". *PAKDD 2003*, LNAI 2637, pp.178–190.

[9] A.I. Vakali. "LRU-based algorithms for Web Cache Replacement", *Lecture Lotes in Computer Science (Volume 1875)*,pp409-418.

[10] H.Bekler,I.Melve. *Survey of Caching Requirements and specification of Prototype*. www.ocguide.com/cache

[11] Jose Borges1 and Mark Levene, "Ranking Pages by Topology and Popularity within Web Sites", *World Wide Web*, Volume 9, Number 3 :2006, pp.301-316.

Mingwu Zhang is currently doctoral student at the College of Software Technology in South China Agricultural University. His research involves both experimental and theoretical study of distributed systems, in general, and trusted computing and web systems, in particular, including distributed middleware systems and advanced embedded systems. His current research interests include performance, scalability, reliability, and security of trusted computing, distributed trust management, as well as mobile and wireless services.

Software Architecture and Parallel Programming Language

The Extension of Petri Nets for Description of Operational Semantics of Flowgraph Stream Parallel Programming Language*

V.P. Kutepov[1], V.A. Lazutkin[2], Liang Liu[3]
Chair of Applied mathematics, Moscow Power Engineering Institute (Technical University)
ul. Krasnokazarmennaya 13, Moscow, 111250 Russia
Email: [1]KutepovVP@mpei.ru, [2]Vilazag@yandex.ru, [3]LiuLiang_pmo@yahoo.com.cn

ABSTRACT

The extension of Petri Nets for the description of operational semantics of flowgraph stream parallel programming language is described in this paper. This language is directed toward large-grained (module) stream programming on cluster systems.

Keywords: FSPPL, FGPP, Operational Semantics, Petri Nets, Parallel programming

1. INTRODUCTION

The purpose of this paper is to construct the formal description of operational semantics execution of flowgraph parallel program (FGPP) on the basis of Petri Nets extension, which possesses the best modeling opportunities for parallel systems. The flowgraph stream parallel programming language (FSPPL) is a realized part of the development system of the flowgraph stream parallel programming for cluster systems under the supervision of Dr. Prof. V.P. Kutepov at the chair of applied mathematics in the Moscow Power Engineering Institute (Technical University) [1]. FSPPL has the following important features: the modularity of its programs, the opportunity of the simple program structuring, and the multilingual programming, applied at the modules subroutines development.

In the first section of this paper the parallel semantics of FSPPL and the its programming features are described. In the second section the extension of Petri Nets language is brought, and with their help the construction of the formal description of parallel operational semantics of FSPPL is introduced.

2. THE DESCRIPTION OF THE PARALLEL OPERATIONAL SEMANTICS OF FSPPL

The first version of the flowgraph language developed in the early 1970s as a result of intensive investigations of parallel systems was designed as a "soft" development of structural (block-diagram) descriptions of serial programs with an intended implementation on multicomputer and/or multiprocessor systems [1, 3]. Henceforth the language was more than once supplemented and extended, and its realizations are developed under various multicomputer and multiprocessor systems. The description of the current version of FSPPL, the tool environment of programming on FSPPL and the execution systems of FGPP are given in [3, 4], and technological aspects of programming on FSPPL are described in [5].

The FSPPL is directed toward large-grained (module) stream programming. Besides the construction of decisions for the computational problems, The FSPPL can also be applied efficiently for program modeling of distributed systems, queuing systems, and others, with interaction between their components being structured and controlled by the dataflows.

The FSPPL allows the following three types of parallelism to be represented in programs efficiently and uniquely:

– a parallelism for data-independent fragments;
– a flow parallelism, conditioned by pipeline data processing;
– a dataset parallelism (i.e. SIMD parallelism) (Single-Instruction, Multiple-Data) implemented in the FSPPL through the tagging mechanism, when one and the same program or its fragment is applied to different data.

Other important (from the programming point of view) features of the FSPPL include the following:
– the possibility of a visual graphical and textual representation of programs;
– the possibility of a simple strategy structuring of programs and reflecting the decomposition hierarchy, which is based on the graph–subgraph relationship;
– the use of conventional sequential languages in module programming.

The parallel execution of the FGPP is represented as a sequence of alternating states, each of which is characterized by a set of processes induced during the execution of the FGPP-module subroutines, which are assigned in the interpretation to their conjunctive input groups (CIGs) [3].

The uniqueness of the relation between input and output values in the parallel performance of the FGPP can be provided through a tagging mechanism [3].

The process of the FGPP execution is conducted according to following rules:

1. A FGPP module is assumed to be ready for running by anyone of its CIGs on the dataset, which is marked by tag T, if all its inputs (in the corresponding buffers) have data marked by the same tag T.
2. If module M is ready to execution by $CIGs_i$ on the datasets, marked by tags $T_1,\ldots,T_k$, k processes, each of which is uniquely identified by the own tag T_i, are simultaneously started on execution.
3. The modules with no-input CIGs (which correspond to subroutines with an empty set of parameters) are assumed to be ready for execution by these CIGs from the time of the FGPP execution initialization; however, the processes induced by them can be generated only once. Thus it is supposed that the subroutines assigned to CIGs with an empty set of inputs operate as generators (either generating data in them or reading them out from some carrier).
4. The process of the FGPP execution is taken to be finished, when any module is not ready to execution and all the processes connected with FGPP execution are completed.
5. In executing a process, its subroutine can use the special-purpose statements *WRITE*, *READ*, and *CHECK*,

*This project is supported by the Russian Foundation for Basic Research (No. 06-01-00817)

which provide an interface between modules (i.e., build various schemes of data exchange between subroutines of different modules through reading or writing data from or to the buffers assigned to the module CIG inputs).

a. The *WRITE* statement conducts write in the giving *output* of the giving conjunctive output groups (*COGs*), with the transferred *value* marked specified *tag*, and has the format: WRITE (<*number of COG*>, <*output*>, <*tag*>, <*value*>).
b. The *READ* statement allows the process to read data with the indicated tag from buffers assigned to the CIG that initiated the process. The data with the indicated tag retrieved from the listed CIG inputs are assigned to variables in the variable process - *input value*. The format of *READ* statement: < *input value* > = READ (<*number of CIG*>, <*input*>, <*tag*>). In the execution of the *READ* statement, if the requested data have not yet arrived to the buffer memory, the execution is delayed until the data arrive. The arrival time is controlled for any recording of data into the buffer memory of the corresponding CIG. When the *READ* statement stops executing, the requested data are deleted from the buffer and the context of the subroutine that induced the *READ* statement is recovered.
c. For a more sophisticated operation with data arriving to module CIGs (in particular, with the assigned buffers), the statement <*availability flag*> = CHECK (<*number of CIG*>, < *input*>, <*tag*>) is provided, which checks the availability of data with the indicated tags at the CIG inputs, and returns *TRUE* as result, if such data is present at the buffer, and *FALSE* – otherwise. This statement allows the process to make an independent decision on its actions depending on the data availability.

Note a number of significant elements of the operational semantics of the FSPPL, which are important for its implementation in parallel systems [3]:

1. The order of execution of the set of processes existing at each step of the FGPP is of no significance; at least, care must be taken by a programmer to make sure that the order would not affect the correctness of the FGPP operation. At the same time, the process scheduling can have a significant impact on the reduction of the FGPP execution time on a parallel system.
2. What processes are ready for execution is determined according to the FIFO principle: the availability of data with the same tag in the CIG buffer memory at all its inputs is checked as the data are written into the buffer memory. Similarly, when the *READ* and *CHECK* statements are executed, the required data are sought in the data buffer as the data are written into it. When the *WRITE* statement is executed, the data are written into the buffer memory as they arrive (in the tail of the data queue).
3. Since one and the same buffer can be operated simultaneously by several processes (reading or writing), such simultaneous actions must be mutually eliminated in the implementation.

3. THE EXTENSION OF PETRI NETS AS THE FORMAL DESCRIPTION MODEL OF THE PARALLEL OPERATIONAL SEMANTICS FSPPL

Petri Nets were developed originally by Carl Adam Petri, and were the subject of his dissertation in 1962 [7]. Petri Nets are the tool of systems research. The theory of Petri Nets makes the system simulation possible by its mathematical representation in the form of Petri Nets. The simplicity of the process modeling of the synchronization, the asynchronous events, the parallel operations, data collision and resource sharing promoted their further development by means of Petri Nets. Petri Nets are mathematical model, which has wide application for the behavioral description of parallel devices and processes. They are successfully used for the modeling and analysis of the parallel systems, the communication protocols, the estimation of the execution and the fault-tolerant systems. The detailed description of the theory of Petri Nets and their application in practice is brought in [7, 8]. Here we shall consider two expansions of Petri Nets: the color token and the generating transitions.

The color token is enough simple and often necessary extended, which was more than once considered with the purpose of the modeling by means of Petri Nets of real processes and their interactions. The essence of the color token is the task of the additional attribute, namely, colors, on which it will be possible to distinguish one token from another. With reference to FSPPL, the color token patterns the mechanism of the data tag.

Generating transitions are necessary for the description of such situations at parallel execution of FGPP, when on CIGs input the data collection (the actual parameters of the subroutine, compared with CIGs) is gathered, marked for one or different tags. In this case, according to the rules of FGPP execution (see section 1), the simultaneous application of the subroutine duplication is probably, which corresponds CIGs to the incoming data on its input.

In order to formally assign this process, we shall compare each CIGs of each module with special transition, which can generate other transitions depending on the data availability of its input. In Fig. 1 there are a) ordinary transitions, as they are interpreted in the model of Petri Nets, and new generating transitions.

Fig.1. Examples of (a) ordinary transitions And(b) generating transitions

Unlike the ordinary transition, which works sequentially if and only if, when in its all input positions there are data (tokens) marked by the same tag (color) and only after operation places in all output positions of data with the same tag (by one token of the same color), the generating transition works by other rules.

If in the all input positions of the generating transitions there is k_i data ($k_i \geq n \geq 1$), the n marks the identical tags $T_1,\ldots,T_n$ (i.e. the CIGs of the module FGPP is ready to execution on n datasets), the generating transition generates the n ordinary transitions, in the each ordinary transition all input positions are located the data marked identical tag T_i, and at the same time these data are withdrawn from the input positions of the generating transition (Fig.2).

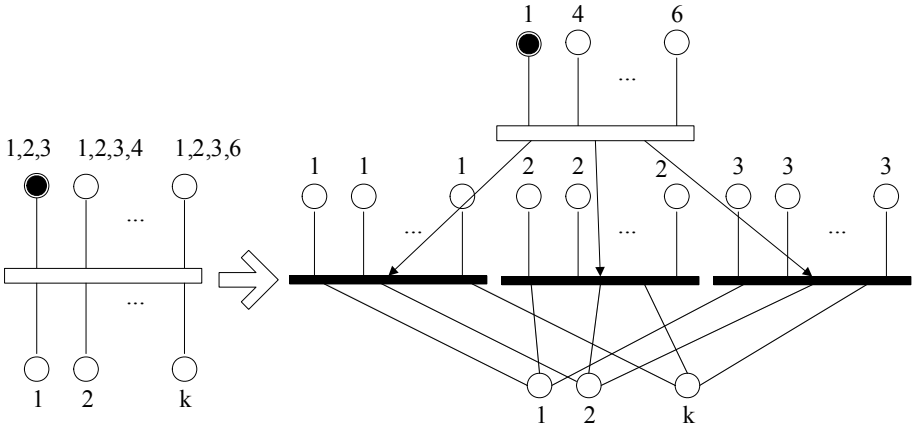


Fig.2. The process of the transitions generation

The generated transitions "keep" the output positions of the generating transition.

The generated transitions, being independent through data, work asynchronously (including simultaneously) as the operation of the ordinary transition after its operation, place in all output positions of the generating transition by one data with the same tag, which has input data.

After the operation, the each generated transition is deleted from the nets with the input positions, and their data have been placed “developed” in the output positions of the generating transition.

It is also assumed that the generating transition asynchronously reacts on the data availability, and every time transitions are generated, if for that the condition of its operation is executed.

Clearly, in the implementation FSPPL the mutual exclusion of the data from any positions of the working transition and the data placement in this positions by another (possibly, this transitions) should be provided. By the way, this requirement is specified in the functioning model of Petri Nets, moreover, all transitions work sequentially because of the input "oracle" operating the transitions, which can work.

In FSPPL during the program execution the definition of the executing subroutine readiness for each CIGs of each module is implemented decentralized, in consequence of that the parallelism, required to the ready simultaneous acquisition for the execution of the parallel processes for various CIGs, is obtained.

According to any model transition defines an opportunity of the operation, this type of parallelism, obliged to simultaneous operation of independent transitions under the condition, if they do not collide, having the general input positions. More precisely, if two transitions have a commonplace, they can work simultaneously if there are the necessary data for them with different tags. There is an example in Fig.3.

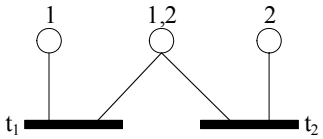


Fig.3. The simultaneous operation of transitions with the general input positions

The transitions t_1 and t_2 can work simultaneously, moreover the t_1 with the input data (1,1), and the transition t_2 with the input data (2,2). In the classical model of Petri Nets such operation is impossible. Either the transition t_1 or transition t_2 can work.

However, it is the theoretical possible to describe the situation for Flowgraph programs, If to assume, that at the execution of some module subroutine in it the *WRITE* statement appears, which simultaneously writes the data 1 and 2 at the input of the transitions t_1 and t_2 (at the input t_1-1, and at the input t_2-2). Modeling this case in details, we shall have a net, which is shown in Fig.4.

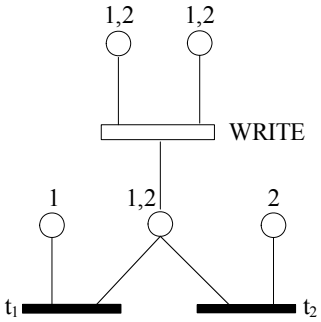


Fig.4. The operation of the generating transition WRITE

Three types of parallelism, presenting in the mentioned modeling description of the execution process FGPP, now have a strict explanation.

The parallelism for data-independent modules (their subroutines) or as it is in [2], the spatial parallelism is the concurrent execution of the subroutines application processes to the incoming data at their inputs.

The SIMD-parallelism, which has place when the same subroutine is applied simultaneously to the various data at its inputs, is expressed in the model through the functioning of the generating transitions.

At last, the multithreaded (owing to the "nonlinearity" of the structure FGPP) pipelined parallelism, when the information coherent sequences of the modules subroutines implement simultaneously various dataflows availability on their inputs.
The *READ* statement arriving at inputs of the data subroutines (CIGs) in FGPP allows to represent adequately flow-dependent computing, and their series computation

($\sum_{i=1}^{n} f(x_i)$, $\prod_{i=1}^{n} f(x_i)$, etc.) are typical examples, which elements come asynchronously sequentially to the processing input of their subroutines FGPP.

The organization of this computing process can be presented in the form FGPP, which is represented in the Fig.5.

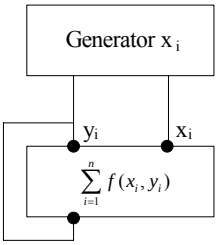


Fig.5. The execution $\sum_{i=1}^{n} f(x_i)$ of FGPP

Here the y_i dummy synchronizing parameter for the function f, defines an opportunity of data reading (the execution of the *READ* statement) from the input buffers of the computing subroutine $\sum_{i=1}^{n} f(x_i)$ under the stipulation that the next x_i arrives.

The index i performs a tag role, and the generator only is in the beginning, "starting" the execution subroutine, assigns the tag, and x and y equal 1. Then before any execution of the *READ* statement the subroutine should transfer the parameter with the tag at the "left" input to per unit more than the previous value y. Thus, the sequential processing (data reading and the computation of the intermediate sum) is implemented, and if to eliminate parameter y_i, all incoming on the processing of the value x_i (with different tags) will lead to that the execution subroutine $\sum_{i=1}^{n} f(x_i)$ should be applied simultaneously to the all arriving x_i, i.e. in the model Petri Nets should compare the generating transition with it.

In Fig. 6 a Petri Net is shown, modeling the *READ* statement. The generating transition t_1 models the execution of the module subroutine (compared with its some CIGs) till the moment of the *READ* statement occurs. At the moment of the occurrence in the subroutine of the *READ* statement module, the conversion to the buffer of the giving module CIGs occurs, and whence it is necessary to consider data. If there are not the required data in the buffer, the process is suspended before their receiving. Thus, the transition t_2 models the data receiving from the buffer and their transfer to the basic computational process, and the transition t_3 is the computational process end of the given module subroutine.

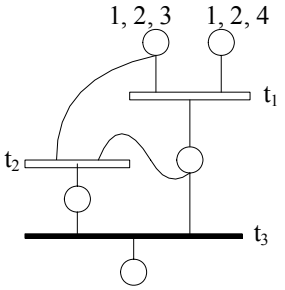


Fig.6. The model of the *READ* statement

It is necessary to note, that in the models of the execution FGPP, the data reading and writing from any input (at any input) should be executed, as the mutually exclusive operations. As the buffer memory is connected with the input, the reading and writing have the sequential execution possibility of the operations to guarantee this mutual exclusion.

Thus the *WRITE* and *READ* statements (including the *CHECK* statement) or should be executed as indivisible, or should be are stipulated the mechanism based on the semaphore technique, having the capability to solve this problem.

4. CONCLUSIONS

In this paper the extension of Petri Nets for the formal description of operational semantics of FSPPL has been described. Note that the description tools for stream computations implemented in the FSPPL have already been used successfully in the development of software for distributed systems: flexible computer-aided manufacturing systems [6], control systems for military operations, etc. It seems likely that they can be competitive for distributive computations represented as object-oriented programs. To do this, it will suffice to compare the UML language and FSPPL in the context of available tools for the description of parallel and distributed data processing.

REFERENCES

[1] V.P. Kutepov, *Arrangement of Parallel Computations in Systems (in Russian)*, Moscow: Moscow Power Engineering Institute, 1988.

[2] V.P. Kutepov, "On Intelligent Computers and Large-Scale Computer Systems of a New Generation," *Journal of Computer and Systems Sciences Internal*, 2003, 35(5).

[3] D.V. Kotlyarov, V.P. Kutepov, M.A. Osipov, "Flowgraph Stream Parallel Programming and Its implementation on Cluster Systems," *Journal of Computer and Systems Sciences Internal*, 2005, 44(1), pp.70-89.

[4] V.P. Kutepov, V.A. Lazutkin, Liang Liu, M.A. Osipov, The Means of Flowgraph Stream Parallel Programming for Clusters,*DCABES2006 PROCEEDINGS "2006 International Symposium on Distributed Computing and Applications to Business, Engineering and Science"*, October 11-15, 2006, Hangzhou, China. Shanghai University Press. Vol. 1, pp. 189-194.

[5] V.P. Kutepov, V.A. Lazutkin, Liang Liu, "The Technological Aspects of Construction of Flowgraph Stream Parallel Programming (in Russian)," in *Proceeding of international scientifically-practical seminar and youth school "High Performance Computing on cluster systems"*, December 12-17, 2006, Saint-Petersburg.

[6] A.A. Tikhonov, *Extended Abstract of Candidate's Dissertation in Technical Science (in Russian)*, Moscow: Moscow Power Engineering Institute, 1989.

[7] DJ. Piterson, "The Theory of Petri Nets and System Simulation (in Russian)," *World*, 1984.

[8] V.E. Kotov, "Petri Nets (in Russian), Science," The main edition of the physical and mathematical literature, 1984.

Reuse-Oriented Software Architecture Design Based on Architectural Meta Model

Ying Shi, Xiaojian Li, Junli Wang, Ying Zheng
State key laboratory of software engineering, Wuhan University, China
Email: lxj0713@tom.com

ABSTRACT

At present, how to reuse design resources on software architecture layer is a difficult problem for academia and industry. This paper presents an architectural meta information model to support reuse, and basing on meta information model of software architecture, gives the implementing frame and view of design tool for reusing architectural design.

Keywords: Architecture Reuse, Meta Information, Tool Support

1. INTRODUCTION

As all we know, software reuse is an important means for improving the efficiency of software development. At present, there are three basic abstract layers for reuse methods. One is *code layer reuse*, that is, reusing source code which has implemented some function. This kind of reuse is not very efficient. Another reuse layer is called *component reuse*. Components encapsulate code module and are placed in a component repository for reuse conveniently. The last layer of reuse is to reuse software system model, that is, the reusable module is the design model of software system. This kind of reuse is really a big-granularity reuse, and we call it architecture *reuse*.

At present, reuse based on software architecture model is rarely researched in-depth in academia and industry. In fact, implementing reuse on such an abstract layer is relatively difficult. The main problems lie in two aspects. First, we should adopt a universal expression of software architecture model, and second, there should have some tools to support reuse of software architecture model at design time. In this paper, we will present the meta model of software architecture and the framework of implementing the reuse of architecture model.

The rest of this paper is organized as follows. First, section 2 explicitly describes the meta information of software architecture, and constructs the meta model. Section 3 gives the general framework of implementing model reuse at design time. Section 4 is about the related work and discussion. And the last part is the conclusion.

2. REUSE-ORIENTED META MDEL OF ARCHITECTURE

We try to identify reuse-oriented meta information at software architecture design time from three aspects. They are static structure, dynamic behavior and architectural reconfiguration. Static structure refers to the elements in the architecture. In the reuse process, these elements and their link information should be explicitly expressed. Dynamic behavior refers to the behavior of architectural elements and the interactions among them. Explicitly describing the behavior can make it clear what and how the reused architecture has been implemented. Reconfiguration refers to changing the static structure when the current architecture can not satisfy new requirements.

For giving a universal meta model of software architecture, we assume that architecture is composed of three basic elements: components, connectors and composites. Composite is composed of component and connector, it can be regarded as a component either.

Component is the computation and data storage unit in a architecture [1], all ADLs describe it as the first element of architecture. For component, we think it includes the following meta information:

Table 1. Structural Meta Information of Component

Name	Content
ID	
Name	
Description	
Interface	Event of interface：Event Property of interface：Property Constraint of interface：Constraint Type of interface：InterfaceType
Property	Name of property：Name Datatype of property：DataType Value of property：Value Type of property：PropertyType
Constraint	Property name of constraint：PropertyName Operator of constraint：Operator Property value of constraint：PropertyValue Type of constraint：ConstraintType
State	Properties in state：Properties Type of state：StateType
Component Type	

And the relationships among these meta-information can be expressed by UML diagram.

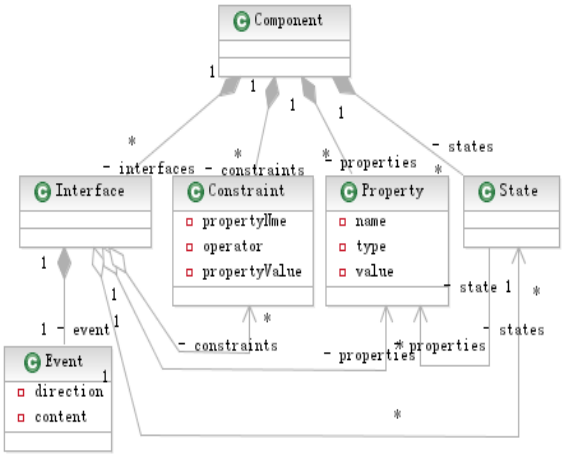


Fig.1. Class diagram of component structural meta-information

And for connector, it has the similar meta information with component, so here we don't list its meta information alone.

And for composite, it describes how the simple component and connector link together to a complex computation unit. It includes the following meta information:

Table 2. Structural Meta Information of Composite

Name	Content
ID	
Name	
Description	
Components	Component Included components
Connectors	Connector Included connectors
Composites	Composite Included composites
Link	source：SourceInterface target：TargetInterface link type：LinkType
Interface	the same as component
Property	the same as component
Constraint	the same as component
State	the same as component
CompositeType	

And the relationships among these meta-information can be expressed by UML diagram

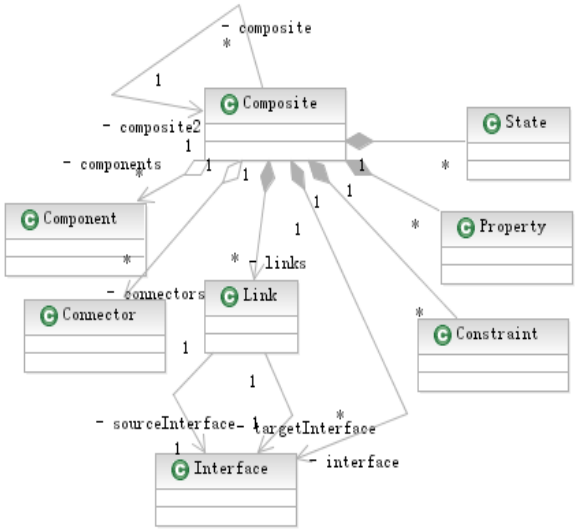


Fig.2. Class diagram of composite structural meta-information

After describing the static structure relationships of architectural elements, we need know the interactions of these elements. The behavior meta information provides much more semantic details for architecture elements.

Here, we adopt a method which is similar with collaboration diagram and state diagram in UML to describe dynamic behavior of component. We regard the mutual relationship between components as collaborations, and collaborations implement a certain functional requirement. The following is collaboration meta information[7][8].

Table 3. Collaboration between Components

Name	Content
ID	
Name	
Description	
Communication	Sender of event in the communication: Source Receiver of event in communication: Target Event in the communication: Event
Sequence	Communication in the sequence: Communication Type of sequence : SequenceType
CollaborationType	

The sender and receiver of event in a collaboration communication are participants, they include the following meta information:

Table 4. Meta Information of Participant

Name	Content
ID	
Name	
Description	
Interface	The same with interface of component
Transition	Prefix condition of state's transition: PreCondition Invariant of state's transition: Invariant Suffix condition of state's transition: PostCondition Start state of participant: StartState End state of participant: Endstate Type of state transition: TransitionType
Participant Type	Entity type in the participant type: EntityType Interface type in the participant type: InterfaceType Transition type in the participant type: TransitionType

And the following is the class diagram of behavior meta information.

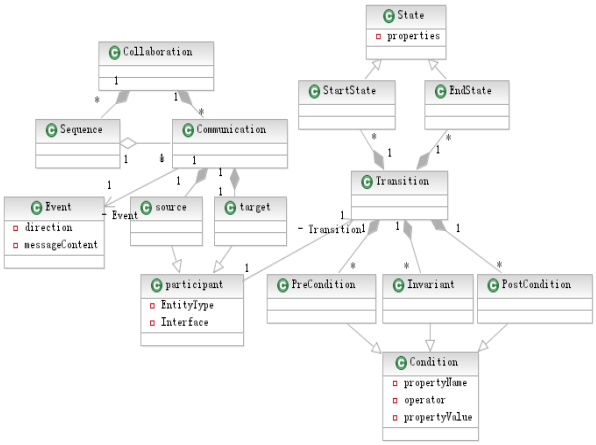


Fig.3. Class diagram of behavioral meta information

For supporting a reuse process, meta operations in architectural dynamic change are also needed. Dynamism has been discussed in many papers[2][3], it is called reconfiguration or reconstruction. In fact, we can differentiate dynamism on three layers. First layer is called interaction dynamism, that is, dynamic communication takes place in a fixed structure. The

second layer is called structure dynamism, the common operations are to construct or delete instances of components or connectors. The third layer is called architecture dynamism, that is, it supports the modifications of architecture infrastructure. On the first layer, there are the following operations like:

a) Add or delete communications in collaborations
b) Add or delete sequences in collaborations
c) Add or delete communications in sequences
d) Modify senders or receives or events in a communication

On the structure layer, there are the following operations:
Instantiate components or connectors
e) Add or delete components or connectors
f) Delete links
g) Replace components or connectors and so on

On the architecture layer, the operations are like: Add, delete, modify the interfaces, interface type, events in interfaces, events' directions, types, attributes, constraints, states of components or connectors or composites

3. SCHEME OF ARCHITETURE REFLECTION

Implementation of reflection is based on meta information, we separate software architecture into two parts: meta-level and base-level [8]. Meta-level includes meta objects which embody meta information, and base-level includes base objects – every component. The scheme is as the following figure:

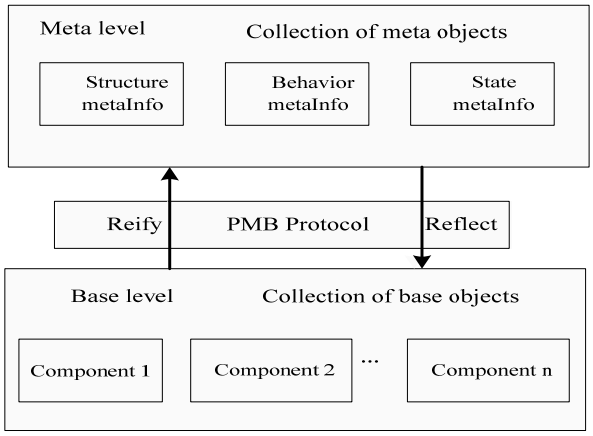


Fig.4. Architecture reflection

In this figure, "PMB protocol" is a Protocol for connecting Meta-level architecture and Base-level architecture, through the PMB, any change of meta object can be reflected to base-level, that is, components can be isolated or replaced, meanwhile , any change of base-level can also be reified to meta-level. For PMB protocol, we can define the following operations on the meta-level side:

1) Initialize(baseLevel): construct meta-level by base-level. This operation serves for reification.
2) getData(): provide information of meta-level.
3) Add(ElementofMetaLevel): add elements in the meta-level.
4) Remove(ElementofMetaLevel): remove elements in the meta-level.
5) Attach(ElementofMetaLevel, ElementofMetaLevel): add a link between two elements in the meta-level.
6) Disattach(ElementofMetaLevel,ElementofMetaLevel): remove a link between two elements in the meta-level.
7) Notify(): send update notification.
8) Destroy(): destroy meta-objects.

On the base-level side, we can define update() operation to modify components, this operation serves for reflection.

4. TOOL IMPLEMENTATION

We are now implementing a design tool for the aim of architectural reuse. the requirements of this tool are as follows:

a) create a new design of architecture
b) edit a design of architecture
c) delete a design of architecture
d) save an architectural design as files
e) save an architectural design into resource repository for reuse
f) drag an architectural design into current design view from repository

The following figure shows the requirements:

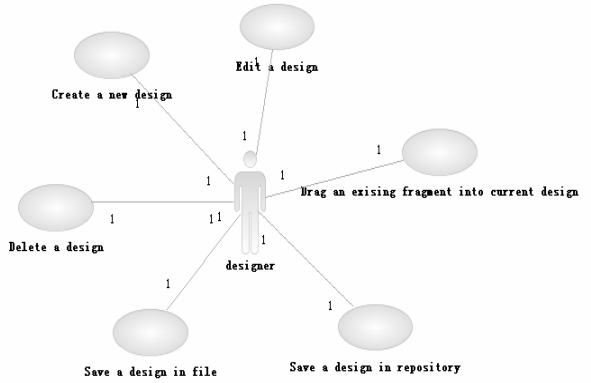


Fig.5. Use case diagram of implementation

For use case of editing a design, we can describe its sub use case as the following diagram.

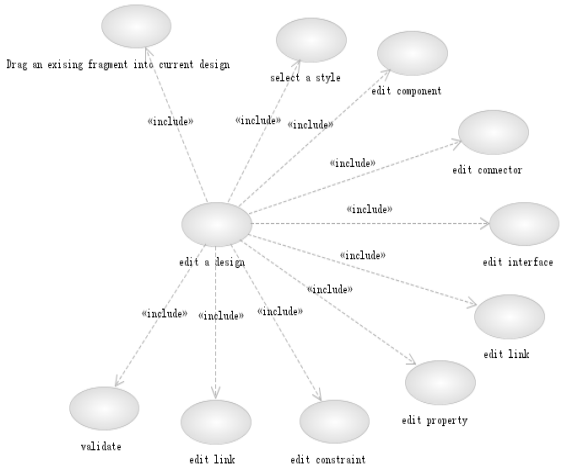


Fig.6. Use case diagram of editing a design

The graphic interface design is as the following:

a) Repository view: reusable resource of architectural design
b) Design view: saving current architectural result
c) Figure view: editing architecture graphically
d) Palette view: dragging design elements into current editor
e) Outline view: showing the breviary graphic of figure view

f) Attribute view: showing and editing attributes of architectural elements

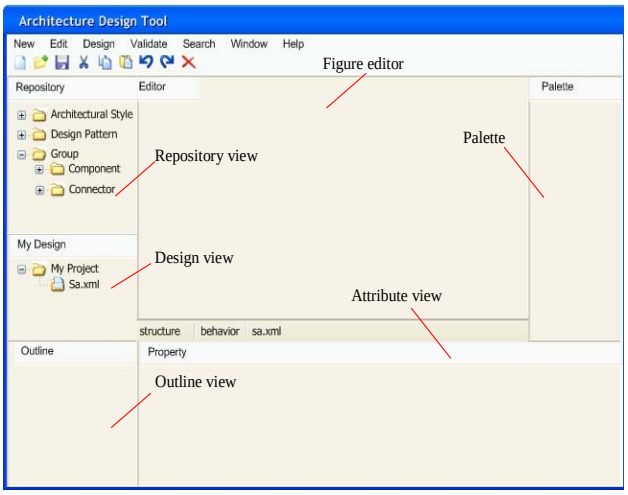


Fig.7. Interface view of implementation

5. RELATED WORK AND DISCUSSION

There are some ADLs(architectural definition language) like xArch[4], xADL[6], xACME[5]. xArch is a set of XML Schema, it defines instances of architecture. And xADL is a development based on xArch. It adds some extensions including types, configurations and implements etc. xACME adds ACME architecture concept such as attributes, constraints and architecture cluster etc. All this work defined some elements of structural aspect of software architecture, undoubtedly, it is very useful for reusing of architecture, but they lack some explicitly description of dynamic behavior, in fact, dynamic behavior meta information is an important part for achieving architectural reuse.

6. CONCLUSIONS

This paper presents a meta model of software architecture which aims to architectural reusing, it is universal and can be used to model software architecture in the architectural design phase. And further more, we give the overall framework and implement view of our tool which support the design and reuse of software architecture. At present, the tool is under developing, after finishing development of the tool, we will do some test and verification work on it.

REFERENCES

[1] N. Medvidovic and R. N. Taylor. “A Classification and Comparison Framework for Software Architecture Description Languages,” *IEEE Transactions on Software* Engineering, vol. 26, pp. 70-93. No.1, Jan 2000.

[2] J. Magee and J. Kramer. “Dynamic Structure in Software Architectures,” Proc. ACM SIGSOFT '96: *Fourth Symp.Foundations of Software Eng. (FSE4)*, pp. 3-14, Oct 1996.

[3] R. Allen, R. Douence, and D. Garlan. “Specifying Dynamism in Software Architectures,” Proc. *Workshop Foundations of Component-Based Systems*, pp.11-22, Sept. 1997

[4] http://www.isr.uci.edu/architecture/xarch/.

[5] http://www.cs.cmu.edu/~acme/pub/xAcme/.

[6] Dashofy, E.M., A.v.d. Hoek, and R.N. Taylor. “An Infrastructure for the Rapid Development of XML based Architecture Description Languages,” In 2*4th International Conference on Software Engineering (ICSE 2002)*. 2002. Orlando, Florida.

[7] R. Allen, R. Douence, and D. Garlan. “Specifying Dynamism in Software Architectures,” *Proc. Workshop Foundations of Component-Based Systems*, pp.11-22, Sep 1997.

[8] C.Cuesta, P. de la Fuente, M. Barrio-Solorzano. “Dynamic Coordination Architecture through the use of Reflection,” *Proceedings of the 2001 ACM symposium on Applied computing*, Las Vegas.

QoS Specification in Software Architecture for QoS-aware applications*

Xiaocong Zhou, Peiyan Li
The Department of Computer Science, Sun Yat-sen University
Guangzhou, Guangdong 510275, China
Email: [1]isszxc@mail.sysu.edu.cn, [2] netfloator@163.com

ABSTRACT

In recent years, QoS-aware applications have become urgently demanded especially in service oriented computing environment. Specifying software architectures of QoSaware applications is not a trivial task because such architectures are complex and dynamic, evolving at runtime according to QoS values and changes. To specify architectures of QoS-aware applications requires to solve two problems i.e. how to specify QoS in the architectures and how to specify the dynamism of the architectures. The dynamism of the architectures can be modeled with primitive actions of Archware π-ADL so our work focuses on QoS specification. In this paper, through defining a QoS enhanced architecture style with π-ADL, we extend π-ADL with QoS specification to facilitate the architecture modeling of QoSaware applications, in which QoS specifications are handled as first class entities. Also, the QoS based architectural mismatch check is developed to detect some QoS violations at the stage of architecture design.

Key words: QoS Specification, QoS-aware, Software Architecture, ADL

1. INTRODUCTION

QoS (Quality of Service), which is relevant to nonfunctional requirement of software, is considerably significant in software development. A high quality software should not only fulfil assigned functions but also satisfy certain non-functional requirements i.e. QoS.

In recent years, QoS-aware applications[10] have become urgently demanded especially in SOC (Service Oriented Computing) environment. They are dynamically composed of QoS-aware components which register their services, engage in QoS negotiation and assemble at runtime according to specific QoS requirements. And in some cases, they must be adaptable and self-configurable to QoS changes.

Specifying architectures of QoS-aware applications is not a trivial task because such architectures are complex and dynamic, evolving at runtime according to QoS values and changes. Traditionally, software architectures are represented with ADLs that provides formal specification for software architectures with basic elements: components, connectors and architectural configurations. But as for QoS aware applications, two key problems should be solved when specifying their architectures.

The first one is how to specify QoS in QoS-aware architectures. Such QoS specifications should be not only nonfunctional constraints of architectures but also what the architectures are ware of, since the QoS values are important parameters for QoS negotiation and architecture evolution. Besides, QoS specification should be able to receive feedback from architectures if architecture evolution affects QoS.

Supported by the National Natural Science Foundation of China under Grant No.60673050

The other problem is how to specify the dynamism of the architecture. To solve this problem requires support for specification of composition and decomposition actions at runtime.

The dynamism of the architectures can be modeled with primitive actions of Archware π-ADL [12, 5, 13] so our work focuses on QoS specification. In this paper, through defining a QoS enhanced architecture style with σπ-ADL, which is the outer layer of Archware π-ADL, we extend π-ADL with QoS specification to facilitate the architecture modeling of QoS-aware applications, in which QoS specifications are handled as first class entities. In our approach, QoS specifications possess first class citizenship [12] i.e. the right to be declared, the right to be assigned, to have equality defined over them, and to persist. Also, we develop the QoS based architectural mismatch check to detect some QoS inconsistencies and violations at the stage of architecture design.The rest of this paper is organized as follows. The next section is devoted to related works and is followed by the background that introduces π-ADL and π-AAL. The fourth section focuses on our approach. Finally, we present conclusions and future works.

2. RELATED WORKS

2.1 QoS Modeling

QoS modeling is discussed in many articles [16, 1, 15, 6, 3, 4]. Most of these QoS models act as design utilities but are unable to be checked automatically. However, in our work, we developed the QoS based architectural mismatch check to detect some QoS inconsistencies and violations at the stage of architecture design. Also, these works integrate QoS models with UML but our work focuses on specifying QoS in software architectures by integrating the QoS model with ADL.

2.2 ADLs

Differences of ADLs have been discussed in the literature [11]. Most of ADLs are concerned about functional features of architectures such as structures and behaviours but ignore QoS aspects of architectures. Some, such as METAH, RAPIDE, ACME, and Weaves, support specification of non-functional properties but the support is rather limited. META-H and RAPIDE only support performance related attributes, such as execution processor , clock period and timing, while our work supports generic QoS attributes. ACME and Weaves allows association of arbitrary annotations with components but they are uninterpretable. In contrast, QoS specifications in our work are checkable.

Besides, π-ADL [13, 5, 12], an innovative architecture description language proposed by Archware European Project, also does not take QoS into account. To overcome this shortcoming, Archware proposes π-AAL[14, 8] to express constraints in architectures. Nevertheless, constraints represented with π-AAL are separate from architecture descriptions and are not accessible by architecture descriptions.

3. BACKGROUND

We choose Archware π-ADL as the basis of our work because of

its express power and extensibility. For one thing, Archware π-ADL supports not only the static configuration of architectural elements but also dynamic composition and decomposition at runtime. In this way, it is suitable for the description of QoS-aware architecture which is a dynamic architecture. For another, Archware π-ADL is defined as a layered language, whose outer layer, called σπ-ADL, provides the style constructs, from which the base componentconnector style and other derived styles can be defined [13]. In Archware approach, when a style is defined, it is possible to associate a new syntax; thus the style provides a more specialized architecture description language [2]. The layered definition of π-ADL also allows to easily extend the type system with new base types and new type constructors [13] so that QoS concepts can be defined as new types with the base types and constructors.

Our work also makes use of π-AAL [14, 8] to implement the QoS based architectural mismatch check[7]. π-AAL is an architecture analysis language based on the μ-calculus in order to specify and support verification of architecture-related semantic properties. In π-AAL, an architectural property is specified in terms of logical formulas comprising: predicate formulas, action formulas, regular formulas, and state formulas.To support π-AAL based verification, Archware provides two verification tools, model checking tool and theorem proving tool.

4. OUR APPROACH

In our work, we extend π-ADL with a QoS specification framework and handle QoS values as first class entities in architecture descriptions. When modeling software architectures, we adopt traditional component-connector view and associate QoS specification with architectural elements such as components, connectors, and ports. Moreover, the QoS based architectural mismatch check is implemented with π-AAL. The rest of this section will explain the above points in detail.

4.1 QoS Specification Framework

Modeling QoS in software architecture is a central concern in this paper. For the sake of defining various QoS characteristics, we utilize in our work a subset of meta concepts presented in [15, 3, 6, 1]. The figure 1 shows the relation of these concepts.

QoS Characteristic, the core concept to build QoS specification, is a quantifiable aspect of QoS, which is defined independently of the means by which it is represented or controlled [9]. *QoS categories,* grouping QoS Characteristics into different subjects, may serve as a hierarchical repository, facilitating the QoS Characteristics to be reused in different projects.

QoS Dimensions are atomic elements to model QoS. A QoS Dimension is determined by its data type, its unit, and the ordering. The data types of dimensions are real, enum and set. The ordering including values of *increasing* and *decreasing* indicates which value is considered a better value. Increasing means that a greater value of the dimension is superior while decreasing means that a lower value is optimal.

Every QoS characteristic is represented by one or more QoS Dimensions. A default dimension of every QoS characteristic is the dimension named *value* which stores the composite value of other dimensions. A key part of a QoS characteristic is a *evaluation* formula serving for evaluate the value of the whole QoS characteristic from its dimensions. Of course, as for the QoS characteristic with only default dimension, *evaluation* formula can be omitted. For example, the QoS characteristic *availability* can be simply modeled by a possibility, or by two dimensions, MTTR (mean time to repair), MTTF (mean time to failure), and a evaluation formula, MTTF/(MTTF+MTTR).

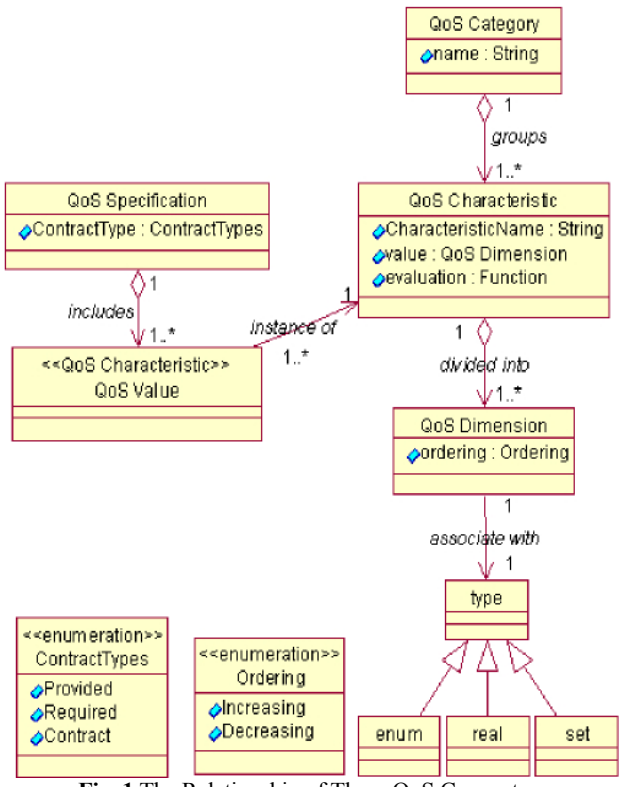


Fig. 1 The Relationship of These QoS Concepts

A *QoS value* is an instance of a QoS characteristic with specific values to its dimensions. And a *QoS specification,* associated with a architectural element, is a set of QoS values. A *QoS specification* is of the type, a required QoS, a provided QoS or simply a contract. A required QoS specifies the QoS that a service requires while a provided QoS specifies the QoS that a service provides. These two sorts of QoS specification are always used to constrain the QoS of ports. And in other situations, a QoS specification is a contract which is the QoS for universal purposes. And the type of *QoS specification* is determined by its attribute *ContractType.*

Syntax of QoS Specification

Framework
QoSCharacteristic::=
id=**QoSCharacteristic** {
dimensionsDef *
}
evaluationDef
evaluationDef::=
ε
| **where**
{**evaluation**={ Expression }}
dimensionsDef::= ε
| *id* =
QoSDimension{dimensionElementsDef}
dimensionElementsDef::= datatypeDef, orderingDef, unitDef
datatypeDef::= **real** | **enum** | **set**
orderingDef::= ε | **Decreasing** | **Increasing**
unitDef::= ε | *"unit name"*, where *unit name* is the name of the unit.

QoSCategory::=
id=**QoSCategory**{QoSQoSCharacteristic^{+}}
QoSSpecificationDef::= {QoSvalueDef*}
ContractTypeDef
ContractTypeDef::= ε
| **where**
{**ContractType**=Required|Provided}
QoSvalueDef::=*QoSCharacteristicRef* =value
| *QoSCharacteristicRef*
{dimensionAssign^{+}}
dimensionAssign::=*DimensionId*=value

The following shows how to combine QoS specification with architecture description.

Syntax of Architecture Description Framework

ArchitectureElement *id* **is abstraction**(parameters)
{
QoS {QoS specification for the component}.
attributes {free variable declarations}.
ports {portDeclaration*}
behaviour {
behaviour described with π-ADL}
}
ArchitectureElement::=**component**|**connector**|**architecture**
portDeclaration::=*id* **is port** {
connectionDeclaration^{+}
} **where** {portQoS}
connectionDeclaration::=**connection** *id* **is in**|**out**(DataType)
portQoS::=QoS **is** *QoSSpecificationId*
QoSSpecificationDef,

Where *QoSSpecificationId* is the hierarchical reference identifier of a QoS specification, the declaring QoS specification inherits all QoS values from *QoSSpecificationId,* and *QoSSpecificationId* can be also empty identifier.

Because QoS specification is accessible in our work, it is essential to develop a mechanism to refer to the values of QoS concepts. The following syntax of references to QoS concepts can be used.

- *id*::**QoS**, where *id* is identifier of an architectural element, refers to a QoS specification associated with an architectural element.
- *QoSSpecRef ::CharacteristicId* refers to a QoS value of a QoS specification, where *QoSSpecRef* is a reference to a QoS specification and *CharacteristicId* is the QoS characteristic name of the QoS value.
- *QoSValueRef ::DimensionId,* where *QoSValueRef* is a reference to a QoS value and *DimensionId* is the name of a QoS dimension, refers to a dimension of a QoS value.
- *ref.AttributeName,* where *ref* is a reference identifier of the above QoS concepts, refers to an attribute of a QoS concept.

4.2 The QoS Based Architectural Mismatch Check

Architectural mismatch is defined by Garlan et al in [7] as "Architectural mismatch stems from mismatched assumptions a reusable part makes about the structure of the system it is to be part of." In the same way, the QoS based architectural mismatch can be defined as that components assume that the environment will provide them services of certain QoS but the environment won't.

The QoS based architectural mismatch check in our work is made at the port level with the help of the QoS specifications associated with ports. It can be implemented with π-AAL. Since the implementation in π-AAL is equivalent to first order logic, we also present the equivalent representations in first order logic to facilitate readers to understand.

π-AAL :
forall x,y:**Port** . connect(x,y) **implies** (x::QoS.ContractType = Provided **and** y::QoS.ContractType = Required **and** conform(x::QoS, y::QoS)) **or** (y::QoS.ContractType = Provided **and** x::QoS.ContractType = Required **and** conform(y::QoS, x::QoS))
First order logic :
$\forall$ x, y:Ports.connect(x, y) $\rightarrow$ (x :: QoS.ContractType = Provided $\wedge$ y::QoS.ContractType=Required $\wedge$ conform(x :: QoS, y :: QoS)) $\vee$ (y :: QoS.ContractT ype = P rovided $\wedge$ x :: QoS.ContractT ype = Required$\wedge$conform(y :: QoS, x :: QoS))

The above formula means that for every two connected ports, if one of them provides a service of certain QoS and the other one of them requires a service of certain QoS, the provided QoS should be better than the required QoS. In this formula, *connect* is a π-AAL predefined predicate to test whether two ports are attached. And *conform* is a predicate with two parameters of the type QoS Specification, which returns true if and only if the first QoS specification is better than the latter one. The implementation of the predicate conform is showed as follows.

conform(x:QoSSpecification, y:QoSSpecification):
π-AAL :
forall a,b:QoSValue . (x-> **includes** a **and** y-> **includes** b **and** a.CharacteristicName = b.CharacteristicName) **implies** (a::value.DataType = Set **and** b::value->**subset** a::value) **or** (a::value.DataType <> Set **and** a::value*a::value.ordering >= b::value*b::value.ordering)
First order logic :
$\forall$ a, b:QoSValues. (a$\in$x $\wedge$ b$\in$y $\wedge$ a.CharacteristicName = b.CharacteristicName) $\rightarrow$ (a :: value.DataType = Set $\wedge$ b :: value $\subseteq$ a :: value) $\vee$ (a :: value.DataType $\neq$ Set $\wedge$ a :: value * a :: value.ordering $\geqslant$ b :: value * b :: value.ordering)

The above formula means that for every pair of QoS values respectively included in the two QoS specifications, which are instances of the same QoS characteristic, the QoS value of the provided QoS should be better than that of the required QoS.

4.3 The Application of the QoS Based Architectural Mismatch Check

The QoS based architectural mismatch check is demanded in many cases. For example, when reusing existing components, to ensure whether the existing components are compatible with the architecture, architectural mismatch check is needed. Obviously, QoS is an significant factor in this check, and the QoS based architectural mismatch check facilitates the component reuse. For instance, a low availability component mismatches with an architecture requiring high availability component and such mismatch will be found out through the QoS based architectural mismatch check. Further, to reuse this low availability component, the high availability architecture with redundant services showed in figure 2 can be utilized. In such architecture, the connector *Redirector* selects an available service from redundant services and redirects requests to it. This enables the *Portal* visits the redundant services in a transparent way.

To specify software architectures for QoS-aware applications, a generic style of QoS enhanced componentconnector view defined by σπ-ADL is presented in this paper, in which QoS values are handled as first class entities. The QoS specifications in this style are not only constraints serving for the QoS based architectural mismatch check but also accessible by architectures as important parameters for QoS negotiation and architecture evolution.

Here is only a first step. More works will be done to refine the QoS model utilized in our work and impose more QoS based constraint on architectures. For example, for a domain specific software architecture, this QoS model will be refined to be more suitable for this domain, and other domain specific QoS based constraint will be imposed on the architecture.

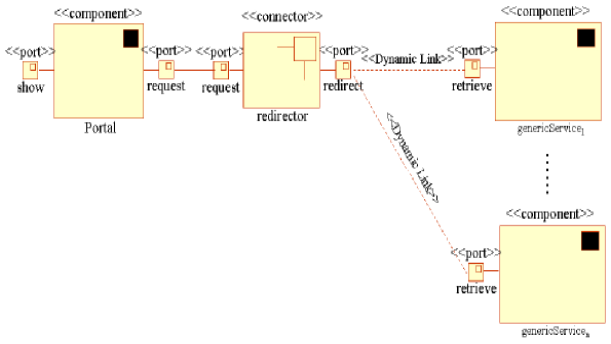


Fig.2. The configuration of the high avail ability Architecture with redundant services

5. CONCLUSIONS AND FUTURE WORKS

To specify software architectures for QoS-aware applications, a generic style of QoS enhanced componentconnector view defined by σπ-ADL is presented in this paper, in which QoS values are handled as first class entities. The QoS specifications in this style are not only constraints serving for the QoS based architectural mismatch check but also accessible by architectures as important parameters for QoS negotiation and architecture evolution.

Here is only a first step. More works will be done to refine the QoS model utilized in our work and impose more QoS based constraint on architectures. For example, for a domain specific software architecture, this QoS model will be refined to be more suitable for this domain, and other domain specific QoS based constraint will be imposed on the architecture.

REFERENCES

[1] K. Chan and I. Poernomo. "Qos-aware model driven architecture through the uml and cim". *In Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference* (EDOC'06), pp.345–354, 2006.

[2] S. Cipan and F. Leymonerie. *Handling dynamic behaviour in software architectures.* In EWSA 2005, volume LNCS 3527, pp.77–93, 2005.

[3] M. A. de Miguel. "General framework for the description of qos in uml". *In Proceedings of the Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing* (ISORC03), pp.61– 68, 2003.

[4] F. Eliassen and Lysaker. Qua: "building with reusable qos-aware components. In Conference on Object Oriented Programming Systems Languages and Applications Companion to the 19th annual ACM SIGPLAN conference on Object--oriented programming systems", *languages, and applications*, pp.154 – 155. ACM Press New York, NY, USA, 2004.

[5] O. F. "The ArchWare Architecture Description Language: Tutorial". *ArchWare European RTD Project*, March 2003.

[6] S. Fround and J. Koistinen. "Quality of service specification in distributed object systems design". *Distributed Systems Engineering Journal*, 5(4), pp.179–202, Dec 1998.

[7] R. O. J. Garlan, D.; Allen. "Architectural mismatch: why reuse is so hard". *IEEE Software*, 12(6), pp.17–26, Nov 1995.

[8] A. I. and G. H. "The ArchWare Architecture Analysis Language: Syntax and Semantics. Deliverable D3".*1b, ArchWare European RTD Project,* IST-2001-32360, Jan 2003.

[9] "International Organization for Standardization". *CD15935 Information Technology: Open Distributed Processing - Reference Model - Quality of Service, iso document iso/iec jtc1/sc7 n1996 edition*, Oct 1998.

[10] D. A. Menasc. "Qos-aware software components". *IEEE INTERNET COMPUTING*, 8(2), pp.91–93, Apr 2004.

[11] M. N. and T. R. *A classification and comparison framework for architecture description languages.*Technical Report UCI-ICS-97-02, Department of Information and Computer Science, University of California, Irvine, Feb 1997.

[12] F. Oquendo. π-ADL: "An architecture description language based on the higher-order typed ~-calculus for specifying dynamic and mobile software architectures". *ACM Software Engineering Notes*, 29(4), pp.1–14, 2004.

[13] F. Oquendo and I. Alloui. The ArchWare ADL: "Definition of the Abstract Syntax and Formal Semantics". *ArchWare Consortium*, Dec 2002.

[14] M. R. and O. F. π-AAL: "An architecture analysis language for formally specifying and verifying structural and behavioural properties of software architectures". *ACM Software Engineering Notes*, 31(2), pp.1–19, Mar 2006.

[15] T. Ritter and M. Born. "A qos metamodel and its realization in a corba component infrastructure". *In Proceedings of the 36th Hawaii International Conference on System Sciences* (HICSS03), pp.10, Jan 2003.

[16] A. Ulbrich and T. Weis. "Qos mechanism composition at design-time and runtime". *In Proceedings of the 23 rd International Conference on Distributed Computing Systems Workshops* (ICDCSW03), pp.118–123, May 2003.

The Approach of Software Component Description based on Ontology *

Xiaofeng Zhou
School of Computer & Information Engineering, Hohai University
Nanjing, Jiangsu 210098, China
Email: zhouxf@hhu.edu.cn

ABSTRACT

Ideally, components should be black boxes, to enable users to reuse them without needing to know the details of their inner structure. So, the description of software component should provide all the information needed by its users. The current description approach of software component apply provider of component to descript their component primarily, but it is very difficult that user of these component use these description to retrieve needed component. This problem will be more and more serious along with surroundings of software component reuse change from centralized to distributed represented Internet. This paper advance an approach of software component description based on ontology to solve problem that user understand these description and get needed component using them exactly in distributed surroundings.

Keywords: Software Component, Component Description, Ontology.

1. INTRODUCTION

Ideally, components should be black boxes, to enable users to reuse them without needing to know the details of their inner structure. So, the description of software component should provide all the information needed by its users. Moreover, this information should be the only information they need[1].
The initial description of component is the syntactic description about component interface what we will call interface specification. Late the semantic description what we call behavioral specification is provided in the literature by way of extended interface specification[2][3]. The description of non-functional properties of software components has recently become a subject of interest[4][5], it is still an open area of research, and uncertain what impact it will have on the future of software component specification.

Now primary approach of component description have 3Cs model[6] and REBOOT approach[7]. More all-around approach have Standardized Specification of Business Component advanced by Component workgroup of Germany Information Society[8][9], Jade Bird Component Model advanced by Peking university[10], and the approach mentioned by Berahne Zewdie[11]. Benneth Christiansson studied 20 different approaches towards software component specification, shown that the main focus in the software engineering community is towards the 'datalogical', and claim that focus should be towards the 'infologic' problem because 1) software component development is about assembly not about construction. This means that we do not have to focus on how the actual development is done; the software component is an existing artifact. 2) Software component development is about acquisition, we need to be able to identify which components we need when assembling systems[12]. So existing approaches just suit that provider of components describe their components, but it is very difficult that user of these component use these description to retrieve needed component. This problem will be more and more serious along with surroundings of software component reuse change from centralized to distributed represented Internet.

This paper advance an approach of software component description based on ontology to solve problem that user understand these description and get needed component using them exactly in distributed surroundings.

2. SPECIFICATION OF SOFTWARE COMPONENT

Aim at need of acquired software component in distributed surroundings, a specification of software component should be consists of domain problem space, interface specification, behavioral specification and non-functional specification. The format is as follows:

Cspec = (DS, Ispec, Bspec, NFspec)

where DS is domain problem space, is the description of knowledge about domain suited by these software components, to help user of these software components understand them easily and correctly; Ispec is interface specification, is the syntactic description about software component interface, is used to describe name, type and property about software component interface; Bspec is behavioral specification, is the semantic description about software component interface, is used to describe inner and external behavioral of software component; Nfspec is non-functional specification, is used to describe the non-functional properties of software component, such as quality property.

2.1 Domain problem space

The domain problem space is background knowledge, set of terms and their correlation organized by form of name space about special application domain. The domain problem space is consisted of general information of domain, type space of function, type space of variable, function space and variable space. The format is as follows:

DS = (Ginfo, FTspac, VTspac, Fspac, Vspac)

The general information of domain is statement about special application domain. The aim is to help their user understand background of these software components. The format is as follows:

Ginfo = (Dname, Dintro, Drelat, Dtime, Dcreater, …)

where Dname is name of this domain; Dintro is introduction of this domain; Drelat is correlative domain, is set of domain name relating with this domain; Dtime is lastly modify time; Dcreater is author of this domain problem space.

The type space of function is a gather of all function types and their properties organized by form of name space about this application domain. Each node in the type space of function includes name of function type, correlative properties and

* This paper is supported by the National Natural Science Foundation of China under the grant No.60573098, 973 project under the grant No.2002CB312002, the Natural Science Foundation of Jiangsu Province of China under Grant No.BK2006168, and the Key(Key grant) Project of Chinese Ministry of Education No.107056.

gather of underling nodes. The format is as follows:

FTspec = {(FTname, FTprop, { LFTname}, …)}

where FTname is name of function type, FTname of the first layer node is FTspec; FTprop is property of this function type, is explain about it in a general way; {LFTname} is gather of underling nodes of this node, the {LFTname} of leaf nodes are NULL.

The type space of variable is a gather of all variable types and their properties organized by form of name space about this application domain. Each node in the type space of variable includes name of variable type, correlative properties and gather of underling nodes. The format is as follows:

VTspec = {(VTname, VTprop, { LVTname}, …)}

where VTname is name of variable type, VTname of the first layer node is VTspec; VTprop is property of this variable type, is meanings about it in a general way; {LVTname} is gather of underling nodes of this node, the {LVTname} of leaf nodes are NULL.

The space of function is a gather of all function, their relations and properties organized by form of name space about this application domain. Each node in the space of function includes function name, function type, function value, function properties and gather of subfunction. The format is as follows:

Fspec = {(Fname, Ftype, Fval, Fprop, { LFname}, …)}

where Fname is function name, Fname of the first layer node is Fspec; Ftype is function type; Fval is function value, it can be NULL; Fprop is function property, is explain about it in a general way; {LFname} is gather of sunfunction name in down-layer, the {LFname} of leaf nodes are NULL.

The space of variable is a gather of all variable, their relations and properties organized by form of name space about this application domain. Each node in the space of variable includes variable name, variable type, variable value, variable properties and members. The format is as follows:

Vspec = {(Vname, Vtype, Vval, Vprop, { LVname, N}, …)}

where Vname is variable name, Fname of the first layer node is Vspec; Vtype is variable type; Vval is variable value, it can be any form such as finite aggregate, area and constant; Vprop is variable property, is explain about it in a general way; {LVname, N} is gather of its members, the LVname is member name, the N is amount of members, the {LVname, N} of leaf nodes are NULL.

2.2 Interface specification

The software component interface specification can be defined specification about its called spot, it is aggregate of description about syntactic of software component, is the most basic description about software component too. The software component interface specification is consist of general information of component, function, perform condition and position primary. The format is as follows:

Ispec = (General, Function, Circ, Position)

The general information of component is universality description about software component, is consist of component name, its name space, its domain problem space, publisher, version and usable information. The format is as follows:

General = (Cneme, Cns, Cds, Publish, Ver, Usable, …)

where Cneme is name of software component, it must named at a name space for ensuring only name; Cns is a name space; Cds is a domain problem space. The functions and input/output parameter of a software component must be described in Cns; Publish is information about provider of this software component, such as manufacturer (name, standard class, contact address), organizer, and so on; Ver include version and data; Usable is usable information of this software component, such as quality, used status and error.

The function information describes function type and correlative input/output parameter type included by this software component, it is core of whole interface specification. The function description includes function name, input port, output port and function explanation. The format is as follows:

Function = {(Fname, Input, Output, Fexp, …)}

where Fname is function name provided by software component. It must be node name of function space in domain problem space belonged this software component; Input is aggregate of input port of this function, each port include port name, port type and port explanation. The port name must be node name of variable space in domain problem space belonged this software component. The port type must be consistent with corresponding node of variable space in domain problem space belonged this software component, or can exchange equally; Output is aggregate of output port of this function, each port include port name, port type and port explanation. The port name must be node name of variable space in domain problem space belonged this software component. The port type must be consistent with corresponding node of variable space in domain problem space belonged this software component, or can exchange equally; Fexp is function explanation.

The perform condition is whole description about perform condition needed by this software component, such as running surroundings (OS, DBMS), program surroundings (program language, class libraries, tools), network surroundings (type, protocol).

The position is description where this software component and correlation matter can be found. It is some pointer or URL what pointes position of software component and correlation matter generally.

2.3 Behavioral specification

The behavioral specification is to describe behavioral of software component. The behavioral specification of software component can be divided into external behavioral specification and inner behavioral specification corresponding because behavioral of software component can be divided into external behavioral and inner behavioral.

The behavioral specification of software component can be looked upon extend of interface specification, used to describe process semantic of software component. It is described by pre/post condition and relation between them and function. The pre-condition is necessary condition that the function is activated, namely the function can execute when all pre-condition satisfy. The post-condition is result that the function execute, namely these post-condition are produced certainly when the function has been activated. The format of behavioral specification is as follows:

Bspec = {(Fun, Pre, Post)}

where Fun is function name, this function must be declared by interface specification of software component, or must be subfunction of function declared by interface specification of software component; Pre is a set of pre-condition; Post is a set of post-condition.

3. DESCRIPTION APPROACH

3.1 Description language and tools

This paper uses OWL, WSDL and OWL-S to describe domain problem space, interface specification and behavioral specification. The tools used this paper include Protégé and own tools.

The OWL Web Ontology Language is designed for use by applications that need to process the content of information instead of just presenting information to humans. OWL facilitates greater machine interpretability of Web content than that supported by XML, RDF, and RDF Schema (RDF-S) by providing additional vocabulary along with a formal semantics. OWL has three increasingly-expressive sublanguages: OWL Lite, OWL DL, and OWL Full[13].

Web Services Description Language Version 2.0 (WSDL 2.0) provides a model and an XML format for describing Web services. WSDL 2.0 enables one to separate the description of the abstract functionality offered by a service from concrete details of a service description such as “how” and “where” that functionality is offered[14].

OWL-S is a OWL-based Web service ontology, which supplies Web service providers with a core set of markup language constructs for describing the properties and capabilities of their Web services in unambiguous, computer-intepretable form. OWL-S markup of Web services will facilitate the automation of Web service tasks, including automated Web service discovery, execution, composition and interoperation. The class SERVICE provides an organizational point of reference for declaring Web services; one instance of SERVICE will exist for each distinct published service. The properties presents, describeBy, and supports are properties of SERVICE.The classes SERVICEPROFILE, SERVICEMODEL, and SERVICEGROUNDING are the respective ranges of those properties. Each instance of SERVICE will present a descendant class of SERVICEPROFILE, be describedBy a descendant class of SERVICEMODEL, and support a descendant class of SERVICEGROUNDING[15].

Protégé is a free, open-source platform that provides a growing user community with a suite of tools to construct domain models and knowledge-based applications with ontologies. At its core, Protégé implements a rich set of knowledge-modeling structures and actions that support the creation, visualization, and manipulation of ontologies in various representation formats. Protégé can be customized to provide domain-friendly support for creating knowledge models and entering data. Further, Protégé can be extended by way of a plug-in architecture and a Java-based Application Programming Interface (API) for building knowledge-based tools and applications.

An ontology describes the concepts and relationships that are important in a particular domain, providing a vocabulary for that domain as well as a computerized specification of the meaning of terms used in the vocabulary. Ontologies range from taxonomies and classifications, database schemas, to fully axiomatized theories. In recent years, ontologies have been adopted in many business and scientific communities as a way to share, reuse and process domain knowledge. Ontologies are now central to many applications such as scientific knowledge portals, information management and integration systems, electronic commerce, and semantic web services[16].

3.2 Description of domain problem space

First we define function type class (FTspac), variable type class (VTspec), function space class (Fspec) and variable space class (Vspec) to express four name spaces of domain problem space. Then we use subclass to define element of each name space.

Each function is defined a subclass, class name is function name, class property is function property, the function is atom function if this class is not subclass, otherwise the function is complex function, the function value is described by ObjectProperty of this subclass, the subfunctions of this function are described by subclass relation. The example of data adding of Stretch water and Drain water like as follow:

```
<owl:Class rdf:about="#StretchDrain">
  <rdfs:comment
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
  >Stretch water and Drain</rdfs:comment>
  <rdfs:subClassOf rdf:resource="#WR_Forecase"/>
</owl:Class>
<owl:ObjectProperty rdf:ID="objectProperty_18">
  <rdfs:range rdf:resource="#StretchDrain_Data"/>
  <rdfs:domain>
    <owl:Class>
      <owl:unionOf rdf:parseType="Collection">
        <owl:Class rdf:about="#Add"/>
        <owl:Class rdf:about="#StretchDrain"/>
      </owl:unionOf>
    </owl:Class>
  </rdfs:domain>
</owl:ObjectProperty>
```

Each variable is defined a subclass, class name is variable name, class property is variable property, the variable type and variable value are described by datatypeproperty of this subclass, the members are described by subclass relation.
For example the variable of gate number is described as follow:

```
<owl:Class rdf:ID="chokeno">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#StretchDrain_Data"/>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:DatatypeProperty
rdf:ID="DatatypeProperty_1"/>
      </owl:onProperty>
      <owl:maxCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >10</owl:maxCardinality>
    </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
      <owl:onProperty>
        <owl:DatatypeProperty
rdf:about="#DatatypeProperty_1"/>
      </owl:onProperty>
    </owl:Restriction>
  </rdfs:subClassOf>
</owl:Class>
<owl:DatatypeProperty rdf:about="#DatatypeProperty_1">
```

```
      <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/
>
      <rdfs:domain rdf:resource="#chokeno"/>
   </owl:DatatypeProperty>
```

3.3 Description of interface

This paper uses documentation, interface, banding and services of WSDL to describe general information of component, function, perform condition and position primary of interface specification of software component.

For example, the function of data adding of Stretch water and Drain water like as follow:

```
<types>
   <xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://wr.example.com/2004/schemas/
resSvc"
      xmlns="http://wr.example.com/2004/schemas/resSvc">
      <xs:element name="StretchDrain_Data"
type="tStretchDrain_Data"/>
      <xs:complexType name="tStretchDrain_Data">
         <xs:sequence>
            <xs:element name="chokeno" type="xs:string"/>
            <xs:element name="logdate" type="xs:date"/>
            <xs:element name="opendoors" type="xs:integer"/>
            <xs:element name="openh" type="xs:double"/>
            <xs:element name="purpose" type="xs:string"/>
            <xs:element name="quantity" type="xs:double"/>
         </xs:sequence>
      </xs:complexType>
      <xs:element name="result" type="xs:boolean"/>
   </xs:schema>
</types>
<interface name = " StretchDrain Interface">
   <operation name="Add"
      pattern="http://www.w3.org/2006/01/wsdl/in-out"
      style="http://www.w3.org/2006/01/wsdl/style/iri">
      <input messageLabel="In"
         element="ghns:StretchDrain_Data"/>
      <output messageLabel="out"
         element="ghns:result"/>
   </operation>
   <operation name="Delete"
      pattern="http://www.w3.org/2006/01/wsdl/in-out"
      style="http://www.w3.org/2006/01/wsdl/style/iri">
      <input messageLabel="In"
         element="ghns:StretchDrain_Data"/>
      <output messageLabel="out"
         element="ghns:result"/>
   </operation>
   <operation name="Modify"
      pattern="http://www.w3.org/2006/01/wsdl/in-out"
      style="http://www.w3.org/2006/01/wsdl/style/iri">
      <input messageLabel="In"
         element="ghns:StretchDrain_Data"/>
      <output messageLabel="out"
         element="ghns:result"/>
   </operation>
</interface>
```

3.4 Description of behavioral

This paper uses precondition and effect of OWL-S to describe pre-condition and post-condition of behavioral specification.

For example, the behavioral description of data adding of Stretch water and Drain water like as follow:

```
<swrl:AtomList/>
<process:AtomicProcess rdf:ID="Add">
   <process:hasPrecondition>
      <expr:SWRL-Condition rdf:ID="Condition_1">
         <expr:expressionObject>
            <swrl:AtomList>
               <rdf:first>
                  <swrl:DatavaluedPropertyAtom>
                     <swrl:argument1 rdf:resource="#chokeno"/>
                     <swrl:argument2
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
                     >1</swrl:argument2>
                     <swrl:propertyPredicate
rdf:resource="http://www.w3.org/2003/11/swrlb#minArgs"/>
                  </swrl:DatavaluedPropertyAtom>
               </rdf:first>
               <rdf:rest>
                  <swrl:AtomList>
                     <rdf:rest
rdf:resource="http://www.w3.org/1999/02/22-rdf-syntax-ns#ni
l"/>
                     <rdf:first>
                        <swrl:DatavaluedPropertyAtom>
                           <swrl:argument2
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
                           >10</swrl:argument2>
                           <swrl:argument1
rdf:resource="#chokeno"/>
                           <swrl:propertyPredicate
rdf:resource="http://www.w3.org/2003/11/swrlb#maxArgs"/>
                        </swrl:DatavaluedPropertyAtom>
                     </rdf:first>
                  </swrl:AtomList>
               </rdf:rest>
            </swrl:AtomList>
         </expr:expressionObject>
      </expr:SWRL-Condition>
   </process:hasPrecondition>
   <process:hasResult>
      <process:Result rdf:ID="Result_1">
         <process:hasEffect>
            <expr:SWRL-Condition rdf:ID="Condition_2">
               <expr:expressionObject>
                  <swrl:AtomList>
                     <rdf:rest
rdf:resource="http://www.w3.org/1999/02/22-rdf-syntax-ns#ni
l"/>
                     <rdf:first>
                        <swrl:BuiltinAtom>
                           <swrl:builtin
rdf:resource="http://www.w3.org/2003/11/swrlb#equal"/>
                           <swrl:arguments>
                              <rdf:List>
                                 <rdf:rest>
                                    <rdf:List>
                                       <rdf:rest
rdf:resource="http://www.w3.org/1999/02/22-rdf-syntax-ns#ni
l"/>
                                       <rdf:first
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
                                       >True</rdf:first>
                                    </rdf:List>
                                 </rdf:rest>
                                 <rdf:first>
                                    <swrl:Variable
rdf:ID="result"/>
                                 </rdf:first>
                              </rdf:List>
```

```
                    </swrl:arguments>
                  </swrl:BuiltinAtom>
                </rdf:first>
              </swrl:AtomList>
            </expr:expressionObject>
          </expr:SWRL-Condition>
        </process:hasEffect>
      </process:Result>
    </process:hasResult>
</process:AtomicProcess>
<swrl:AtomList/>
```

4. RELATED WORK

Claus Pahl[17] use description logics, which underlie Semantic Web ontology languages, such as OWL, to develop an ontology for matching requested and provided component. [18] introduces an ontology that in particular provides a rich reasoning framework for behavioural aspects of Web services or, indeed, components on the Web.

Antonia Albani and Jan L.G. Dieta[19] introduces a process for the identification of business components based on an enterprise ontology, being a business domain model satisfying well defined quality criteria.

Peng Xin[20] introduces ontology to act as the common base of reuse requirements and component representation on the basic of the facet-based approach, so that they can match on the semantic level. Upper ontology and domain ontology are also introduced to support the description of domain-specific features.

5. CONCLUSIONS

Existing approach of software component description aim at centralized component library basically, so they consider coincidence problem of description semanteme rarely. This problem will be more and more important along with surroundings of software component reuse change from centralized to distributed represented Internet. This paper introduces domain problem space, uses form of name space to describe standardization definition of semantic information of functions and variables in domain using software components, solves the coincidence problem of description semanteme surroundings of distributing, establishes base for matching and retrieve of software component in distributed surroundings.
In addition it can be realized completely using description framework provided by domain ontology to describe domain problem space of software component because the technologies, such as domain ontology, grow up. It will be more easy that user understand and use software components well and truly.

REFERENCES

[1] F. Lüders, K.-K. Lau, and S.M. Ho, *Specification of Software Components, Building Reliable Component -based Software Systems,* Chapter 2, pages 23-38, Artech House, 2002.

[2] Frantisek Plasil, "Behavior Protocols for Software Components," IEEE Tran. *On Software Engineering,* Vol. 28(11), pp 1056-1076, 2002

[3] Frantisek Plasil, "Enhancing Component Specification by Behavior Description- the SOFA Experience," *Proceeding of WISICT05,* 2005.1

[4] Jianwen Zhu, Wei Sum Mong, "Specification of Non-Functional Intellectual Property Components, Proceeding of Design," *Automation and Test in Europe Conference and Exhibition* (DATE'03), pp. 10456-10461, 2003

[5] Steffen Zschaler, "Towards a Semantic Framework for Non-functional Specifications of Component-Based Systems," *Proceeding of 30th EUROMICRO Conference* (EUROMICRO'04), pp. 92-99, August 2004

[6] Latour L., Wheeler T., Frakes B., Descriptive and prescriptive aspects of the 3Cs model: SETA1 working group summary, CASE Centre, Syracuse University, New York: Technical Report 9014, 1990

[7] Guttorm Sindre, Reidar Conradi, "The REBOOT Approach to Software Reuse," *Journal of Systems and Software,* 1995, 30:201-212

[8] Jörg Ackermann, Klaus Turowski, "Specification of Customizable Business Components," *Proceedings of the 29th EUROMICRO Conference*(EUROMICRO'03), pp391-394, 2003.9

[9] K. Turowski, (ed.), "Standardized Specification of Business Component," February 2002, http://www.fachkomponenten.de

[10] Li Keqin, Guo Lifeng, Mei Hong, Yang Fuqing, An Overview of JB (Jade Bird) Component Library System JBCL, Proc. TOOLS Asia '97, Sep. 1997

[11] Berahne Zewdie, C.R.Carlson, "Essential Parameters for Component Specification," *Proceeding in SERP'04,* 2004.6.24

[12] Benneth Christiansson, Marie-Therese Christiansson, "The Missing Approach for Component Specification," *Proceeding in 1st International Workshop Component Based Business Information System Engineering,* 2003.9.2

[13] http://www.w3.org/TR/owl-features/

[14] http://www.w3.org/TR/2006/CR-wsdl20-20060327

[15] http://www.w3.org/Submission/OWL-S/

[16] http://protege.stanford.edu/

[17] Claus Pahl, "An ontology for software component matching," *proceeding of Fundamental Approaches to Software Engineering FASE'2003,* pp: 208-216, 2003

[18] Claus Pahl, "Ontology-based Description and Reasoning for Component-based Development on the Web," *proceeding of ESEC/FSE Workshop on Specification and Verification of Component-based Systems SAVCBS'03,* Helsinki, Finland. pp. 84-87. September 2003.

[19] Antonia Albani and Jan L.G. Dieta, "Identifying Business Components on the basis of an Enterprise Ontology," *proceeding of First International Conference on Interoperability of Enterprise Software and Applications Interop-ESA 2005,* pp. 335-348, 2005

[20] Peng Xin, Zhao Wen-yun and Xiao Jun, "Representing and Retrieving Components Based on Ontology," *Journal of Nanjing University,* Vol. 40(10): 470-475, 2005

A Study of Network Component Migration via Reflection

Jubo Luo[1,2], Wei Liu[3], Junfeng Yao[1], XiaoJian Li[1], Dan Xie[1]
[1]State Key Laboratory of Software Engineering (Wuhan University)
Wuhan 430072, China
[2]School of Management, Wuhan University of Science and Technology
Wuhan, 430081, China
[3]School of Computer, Wuhan University of Technology
Wuhan, 430063, China
Email: whuluocheng@126.com

ABSTRACT

Resources on the internet are not subject to centralized control and grid resources are distributed, their availabilities may be very dynamic. Most recently, wide-area networks have presented a huge potential for migration. Migration of individual components can be an effective strategy for dealing with dynamic resource availabilities.However, migration of components that are part of a distributed application is complicated due to the possible interactions between them. We present an approach for migration of distributed components via reflection, in the presence of communication between them. There are explicitly a meta-level space and a base-level space in the reflective architecture.The elements in the meta-level monitor the elements in the base-level, and control the base-level components with some strategies in the reflective architecture. This paper focuses on network component migration via reflection.It gives the Meta-model of distributed network architectures. In addition, it defines the network component migration and migration process based on reflection. And a scenario example of network component migration depicted by these notations is presented to show the applicability. Finally it comes the sum-up and some further works.

Keywords: Reflective Architecture, Meta-level, Base-level, Network Component Migration

1. INTRODUCTION

Network resources are not subject to centralized control and grid resources are distributed, their availabilities may be very dynamic. Most recently, wide-area networks have presented a huge potential for migration. Migration of individual components can be an effective strategy for dealing with dynamic resource availabilities. However, migration of components that are part of a distributed application is complicated due to the possible interactions between them. We define component migration as the movement of a component instance from one host to another in a distributed system. A component can be migrated from a host with a relatively high load to one under a lower load to improve the application's performance.

The reflective architecture explicitly divides a system into two different spaces [1], one is base-level architecture and the other is meta-level architecture. The base-level is the traditional architecture, which describes how to realize application logic and functional requirements of software system as well as the distribution plan of responsibilities and tasks. Meta-level architecture describes the relevant information of base-level architecture, e.g. topology of base-level architecture as well as components and connectors included in base-level architecture.

In this paper we are mainly concerned with network component migration via reflection.In section 2, we present the Reflective Architecture.In section 3, we propose model of distributed network architectures. .In section 4, it defines the network Component Migration Service and Migration Behavior based on reflection. In section 5, a scenario example of network component migration depicted by these notations is presented to show the applicability. Finally it comes the sum-up and some further works.

2. REFLECTIVE ARCHITECTURE

During the dynamic design of software system, we will use meta information in order to manage, control and use a software system more simply, flexibly and automatically. Meta information is the information about information, which can describe structure, semantic, purpose and usage, etc. of information. Reflection is a technology closely related to meta information. Reflection manages and controls information by meta information. Therefore, we add reflection mechanism into the architecture to build a reflective architecture.

There are explicitly a meta-level space and a base-level space in the reflective architecture. The elements in the meta-level space and the base-level space are interrelated and interactive during operation in the reflective architecture. Fig.1 is the schematic diagram of reflective architecture.

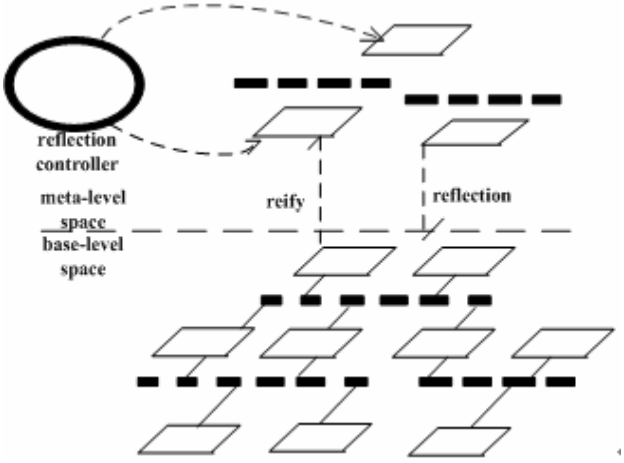


Fig.1. Diagram of Reflective Architecture

The elements in the meta-level monitor the elements in the base-level, and control the base-level components with some strategies in the reflective architecture [3]. The system

reflection controller controls composition, configuration and interaction of the whole system in the reflective architecture. In the meanwhile, it can be called by the external and makes these changes effective during operation. It consists of the following parts:

(1) The list of base-level and meta-level elements and corresponding relations.
(2) Topology of base-level components and connectors.
(3) Reflection and reify strategies of meta-level and base-level.

3. MODEL OF DISTRIBUTED NETWORK ARCHITECTURES

In section 2, we present the Reflective Architecture. In this part, a distributed system may consist of heterogeneous machines connected with heterogeneous networks, and the networks may be shared. In many distributed systems only data maybe transferred between the nodes. Other systems allow the site of execution of a process to be changed by transferring the relevant information from one host to another.

A node is an object defined in ProActive whose aim is to host several active objects. It provides an abstraction for the physical location of a set of active objects. An active object can be bound to a node either at creation time or as the result of a migration.[12]
An example of a distributed architecture is depicted in Fig.2-(a)(b) which shows networks in a hierarchical structure (each network can have many subnets and only one supernet), nodes belonging to networks, and objects distributed on nodes.

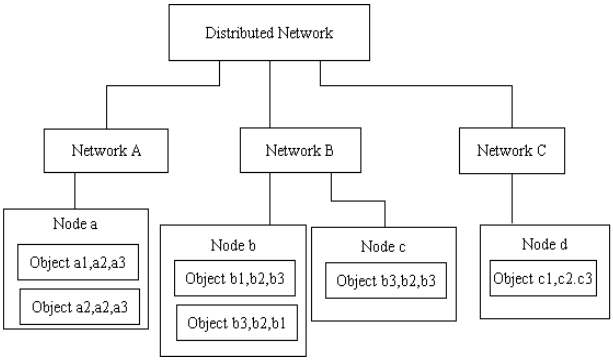


Fig.2.(a) An example distributed network architecture.

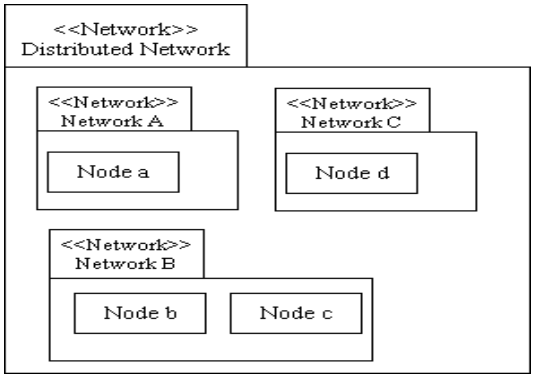


Fig.2.(b) An example Network Deployment Diagram .

4. NETWORK COMPONENT MIGRATION

A network component can be migrated from a host with a relatively high load to one under a lower load to improve the application's performance.In this way, we can improve the overall system performance.

We define component migration as the movement of a component instance from one host to another in a distributed system. A component can be migrated from a host with a relatively high load to one under a lower load to improve the application's performance.In this way, we can improve the overall system performance.

A component can be migrated to another host to ensure that the component survives the shutdown or removal of its current host from the application. Each migration task is concerned with two objects: the source object and the target object. The migration step is specified by giving the modifications that have to be performed in order to turn the source object into the target object.

Definition1 (NetworkComponent Migration Process): A system, Sys, has Migration Process with respect to MigrationProcess : Act x $Node_o$ x $Node_d$→ Act_s, and remote creation request function, RemoteRequest: (act, $node_o$,$node_d$) →Message, is called migration processes.

A migration request is given by a pair (act, $node_o$,$node_d$) where act∈Act_s identifies the actor to be migrated, and $node_o$ is the original $node_d$ is the destination node. This is interpreted as a request to move the computation carried out by act to node. By suspending computation of the actor to be migrated, and noting its current description to determine the computation to be migrated. Then, arrange for any messages that arrive for the migrated actor after its suspension to be rerouted to the actor created to carry on its computation[5][10].

Process migration is the act of transferring a process between two machines (the source and the destination node) during its execution. Some architectures also define a host or home node, which is the node where the process logically runs. The source object and the target object are represented by the design documents that must be produced during the design process. The design documents are organized as a hierarchical, modrdarly structured description of the object in terms of a multi level hierarchy of components and relationships between them. A component may be a primitive or it may be a modular,hierarchical design document[13].

Migrating one component may have an adverse effect on other components that are communicating with it. Hence, the said policies would have been evaluated for the whole application, and not just for individual components. The framework has to ensure that the components are scheduled such that all the policies are satisfied simultaneously.

5. A SCENARIO EXAMPLEOF NETWORK COMPONENT MIGRATION

In previous parts, we present the Reflective Architecture and Meta-model of distributed network architectures. And in section 4, it defines the network Component Migration Service and Migration Behavior based on reflection. In this part, a scenario example of network component migration depicted by those notations is presented to show the applicability.

In order to migrate an individual component to another resource, all communication with that component is halted, the component is migrated, the migrated component is rediscovered by the other components, and all communication to the component is resumed [11]. The migration process is divided in some stages, each one having a finite set of steps, representing a total amount of 12 steps (Fig.3).

Migration processes are migrated by the system, either semiautomatically or automatically, from overloaded processors to idle or underloaded processors to achieve equitable distribution of workload, possibly leading to faster completion of the task.

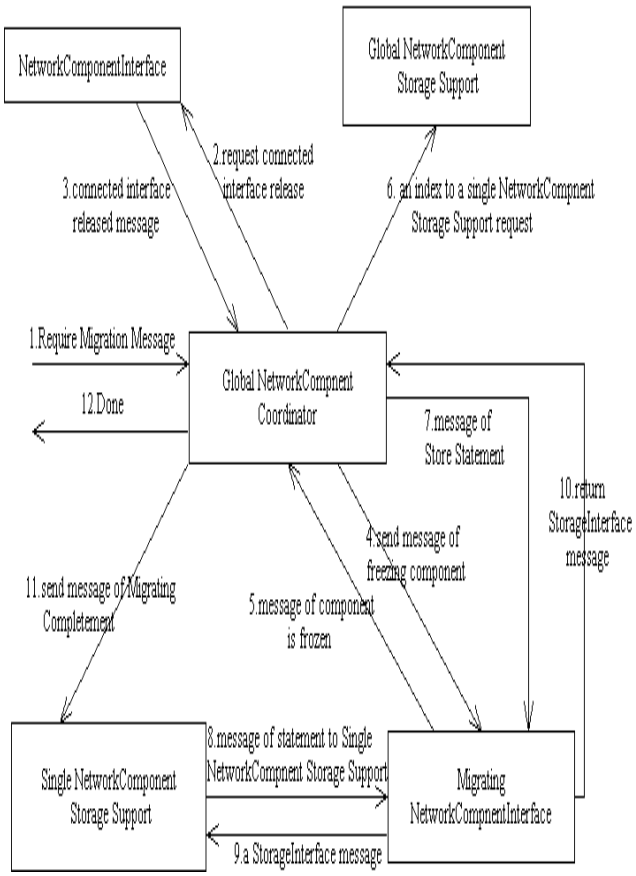


Fig.3. An example of network component migration process

An end-user initiates migration of a component by invoking the migrate Component method on the Application Coordinator.Using the references for all the components that are part of the distributed application .The Global NetworkComponent Coordinator sends a request message to the required NetworkComponentInterface. The process state is typically retained on the source node until the end of migration. State is transferred and imported into a new instance on the remote network node. Once all of the state has been transferred from the original instance, it may be deleted on the source node. A migration request is issued to a remote node. A process is detached from its source node.Communication is redirected by queuing up arriving messages directed to the migrated process.After receiving migrationYES messages,the Global NetworkComponent Coordinator is to migrate the SingleNetworkComponent. Dynamic migration involves briefly locking the progress of the unit of migration, moving the migration unit to a destination system, implementing one of several mechanisms for rebinding references, and finally resuming execution. On receipt of the lock component request, the NetworkComponentInterface waits till all remote invocations are complete [6].

Accessing more processing power is a goal of migration when it is used for load distribution.Exploitation of resource locality is a goal of migration in cases when it ismore efficient to access resources locally than remotely. The NetworkComponentInterface sends the interfaceID to the Global NetworkComponent Coordinator as part of the component situation message. Moving a process to another end of a resource sharing is enabled by migration to a specific node with a special hardware device, large amounts of free memory, or some other unique resource. The NetworkComponentInterface get the state of the component from the right Individual Storage service support, and sends a yes message to the Global NetworkComponent Coordinator.

6. CONCLUSIONS AND FUTURE WORK

This paper focuses on network component migration via reflection. It gives the Meta-model of distributed network architectures. In addition, it defines the network Component migration service and migration process based on reflection. And a scenario example of network component migration depicted by these notations is presented to show the applicability.

Through the study and use of component migration in real applications we plan to determine which of these policy decisions are best automated and which are better left under user control. One of our long term goals is to move to a reflective architecture that provides an unbounded number of meta-levels with a single basic mechanism. The challenge here is to develop easy to use principles for harnessing the power of reflection and avoiding the potential chaos that is possible with its unrestricted use.

Most recently, wide-area networks have presented a huge potential for migration. The literature on process migration is extensive. However, these research efforts are primarily driven by the need to balance load on parallel processor networks. Process migration will continue to attract research independently of its success. In market deployment. The most promising new opportunity is the use of mobile agents in the Web. Mobile agents bear a lot of similarity and deploy similar techniques as process migration. The lower cost/benefit ratio associated with introducing migration to component based systems may mean that component relocation is the problem that process migration techniques have been looking for.

REFERENCES

[1] Rui Jorge da Silva Moreira, “Framework Of Reflective components for Managing architecture Adaptation,” Lancaster University, UK, Doctor Thesis, Oct 2003.

[2] ZaoQing Liang, Shi Ying, Rongzeng Cao, XiangYang Jia, Zhang Tao, “Reuse Software Architecture through Dynamic Composition,” The *IFIP International Conference on Research and Practical Issues of Enterprise Information Systems*, April 24-26, 2006. Vienna, Austria, pp.297-306.

[3] Yu Xiao-feng, Ying Shi, Jia Xiang-yang, Zhang Tao, “A

reflection-based analysis and design method for non-functional feature," *Computer Engineering*, 32(9), May, 2006, pp.91-93.
[4] Vahid Garousi, Lionel C. Briand and Yvan Labiche, "Traffic-aware Stress Testing of Distributed Systems Based on UML Models," *ICSE'06*, May 20-28, 2006, Shanghai, China.
[5] Nalini, Carolyn Talcott, "Reasoning about Meta Level Activities in Open Distributed Systems," *PODC 95* ,1995 ,ACM
[6] Sriram Krishnan, "An architecture for checkpointing and migration of distributed component on the grid," Dissertation of PH.D, Indiana University, 2004.
[7] European Information Society Technologies, "Component Based Open Source Architecture for Distributed Telecom Applications," in http://coach.objectweb.org, 2003.
[8] D. Gannon et al. "Programming the Grid: Distributed Software Components, P2P and Grid Web Services for Scientific Applications," In *Special Issue on Grid Computing, Journul of Cluster Computing*, July 2002.
[9] G. Stellner. CoCheck: "Checkpointing and Process Migration for MPI," In *10th Internutionul Purullel Processing Symposium*, 1996.
[10] R. Wolski, N.T. Spring, and J. Hayes. "The Network Weather Service: A Distributed Resource Performance Forecasting Service for Metacomputing," *Journul of Future Generation Computing Systems*, 1999.
[11] Foster, C. Kesselman, J. Nick, and S. Tuecke. "Grid Services for Distributed System Integration," *Computer* 35(6), 2002
[12] Baomin Xu, Weimin Lian*, Qiang Gao, "Migration of Enterprise JavaBeans with ProActive Interposition Objects," volume 38(8), August 2003,ACM
[13] Rainer Briick,Migration: "A Model for Design by Modification,"1993,*ACM*

Jubo Luo is presently a PhD student in the State-Key Lab.of Software Engineering, WuHan University, Wuhan, China. His research interests in software engineering include component based software development, software component software architecture, software reuse.

The Principle of Flexible Composition of Software Component in Domain*

Ping Ai[1], Yali Chen[2]
[1]State Key Laboratory of Hydrology-Water Resources and Hydraulic Engineering, Hohai Univ., Nanjing, 210098, China
[2]The Bureau of Hydrology, Yangtze River Water Resources Commission，MWR，Wuhan, 430010, China
Email: aip@hhu.edu.cn

ABSTRACT

The application system of computer for a specific domain has become an important part of business systems in such domain. However, it is now quite difficult to directly apply the results from the research on software component to a specific domain due to inadequate research aims at characteristics of application. Based on a comprehensive survey of the concept component, domain component, application framework, the behavior of the component, the flexibility and the flexible composition of the component, this paper elucidates the principle of flexible composition for domain component.

Keywords: Software Engineering, Principle of Flexible Composition, Analysis, Domain

1. INTRODUCTION

The development and application of computer system for a specific domain requires the software development can not only satisfy the requirements of standardization design and large-scale production but also provide integrated services and can be configured on needs. Therefore a research on software component technology should be conducted to improve the capability of application system as well as reduce development risk and cost for maintenance.

Software component technology has been researched and developed since McIlroy [1] put forward the concepts of component and component factory in 1968. Generally speaking, software component is a unit of software, which is developed independently with specific functions and is used to assemble an application system together with other components and supporting environment. A software component has three key characteristics: encapsulation, reuse and composition. Encapsulation means a component is a prefabricated knowledge services. Reuse means software can be used repeatedly due to component. Composition means a component is not a complete application program.

Component composition is the core of component-based software development. At present, depending on how much is known about the internal details of components, there are three methods of component composition: Black-box, White-box and Grey-box. Grey-box method is now the focus and a lot of relevant foundation researches have been completed. For example, Guijun Wang presented component composition framework for OO distributed systems [2]. Fabio Kon proposed component configuration framework [3]. A. P. Barros discussed the framework of workflow for B2B component assembly [4]. John Penix presented a framework for component automatic configuration and integration [5]. Bridget Spitznagel presented the connector model and a compound approach for constructing connectors [6]. Zhong Wang proposed an object-oriented architecture based on multi-agent adapter [7]. Uwe Abmann also presented a composition approach based on meta-programming grey-box connectors [8]. All of these examples use grey-box composition method.

Although significant development has been achieved, it is quite difficult to directly apply these results to specific domains due to inadequate research on the characteristics of application in the specific domain.

Components at different levels all require flexibility for composition. Comparing with the components at other levels, the code component is the most difficult component for flexible composition. This paper puts focus on the flexible composition of code component, therefore all of the word "component" in this paper refer to code component unless it is noted specifically.

Some key issues about the application of component technology in specific domain are discussed in section 2. Section 3 puts forward some concepts including concept component, domain component and so on. Section 4 presents the technical principle of flexible component composition. Conclusions are drawn in section 5.

2. DOMAIN CHARACTERISTICS AND COMPONENTS COMPOSITION

Domain refers to scope, departments or industries conducting specific activities, e.g. the domain of water resources. Specific domain is the concept of a single domain. In another word, specific domain limits the scope of computer applications. As a component is a logic segment of business application in the specific domain, a difficulty of component design is how to define this logic segment. The diversity and complexity of business logic as well as various structure of application system's platform make it is difficult to implement the application of whole business by composing a set of non-configurable components, which can even not adapt to a minor change on the business logic. Therefore, components for a specific domain should be flexible for composition and can adapt to business changes within a certain extent.

Among various application systems for a specific domain, there are always a large number of modules with same function. With the popular application of computer in domains, many issues about software development and maintenance emerged. Users often complain that the software is too expensive and updating is too fast. Moreover, it is hard to modify the software when business logic changed. Therefore one of the effective ways to resolve the issues existing in the software is to improve the flexible reuse level of components

* Supported by the National High-Tech Research and Development Plan of China under Grant No. 2005AA113150; the Key Project of Science and Technology Research of the Ministry of Education of China under Grant No. 107056

by widely applying flexible component technology especially in the development and maintenance of application system for specific domain.

The current research on component technology shows that there are great difficulties in widely applying component technology in specific domain mainly because the theoretical system of component technology needs to be further improved while researchers still focus on resolving the basic problems of component technology.

However when component technology is connected with specific domain, many basic problems can be simplified. For example, the rational granularity of component has close relationship with business logic of domain. Likewise, discussion on the flexible composition of components in general cases will make the problems more complicated.

The application basis of component technology in specific domain is to establish supporting system for component technology at each link of software development and maintenance. Component composition technique involves in all aspects of component technology. As a result, component composition, the flexible composition in particularly, has become the key factor to ensure the success application of component technology in specific domain.

The Grey-box method is used for flexible composition of component. No matter the method is based on framework, connector or glue codes, the core of composition methods is to solve the configuration of interface. It can even realize the connection of interfaces by adding codes during component composition. Because most of these researches are conducted without clear application background, it is difficult and complicated to apply these methods in specific domain.

(i) For application in the specific domain, many basic characteristics of component can be objectified, such as the encapsulation and relative integrality of components, so that the complexity of interfaces can be reduced to simplify the composition of components.
(ii) Although components, objects, modules and functions share many common characteristics, some differences also exist among them. The uppermost difference is that component is designed and developed for the purpose of composition. However, current researches don't highlight this characteristic of component and have various understanding on the composition, which is adverse to the development of application in domains.
(iii) For application in specific domain, standardization and specification could solve the problems of matching and description for part of factors related to component composition.

The flexible composition of component in specific domains is constrained by the business features of domain.

3. BASIC CONCEPTS

Definitions are given to some basic concepts in order to explain flexible composition of components in domain and its technical principal.

3.1 Concept Component

Software is composed of programs and documents concerned in the computer system. A program is the description of processed objects and processing rules of computer. A document is the necessary explanation of program [9]. As part of software, component is composed of programs and documents concerned, which is part of processed objects and processing rules.

The concept of component is relative to the unit of software containing components, which has to follow some stipulations:

(i) A component is composed of binary source codes package and relevant documents;
(ii) In order to clarify the concepts of software and program, it stipulates that the components forming software should include documents while the components forming program shouldn't include document. Furthermore, the composition of software should include integration of documents while the composition of program shouldn't include integration of documents;
(iii) A program should include at least one framework component and one non-framework component in order to avoid nested definition on component and main body;
(iv) There are many types of composition for components, but no one could directly modify the source codes of component. Moreover the same component can be used by many times as required during the composition of one program;
(v) The process of computing business objects in accordance with corresponding rules is called business logic. Business logic can be separated into several relatively independent sub-logics. In this way, program can be regarded as implementation of business logic and component can be regarded as implementation of the sub-logics.

Definition 3.1 (concept Component, cC) Concept component is a unit of program composed of many computer instructions to implement the specified sub-business logic.

Definition 3.2 (Component Set, CS) Component set is a numerable collection of components. Concept component set (cCS) is also a numerable set, which is:

$$|cCS| = N, N < \infty \quad and \quad ((i \neq j) \leftrightarrow (cC_i \notin cC_j)),\ i, j \in \{n \mid 0 < n \leq N\}$$

Definition 3.3 (granularity of component) Granularity of component refers to the length of sub-business logics realized by components, in another word, it is the number of instructions contained in component. Appropriate granularity of component depends on the application characteristics of domain.

Definition 3.4 (Environment of Component) Environment of component refers to the collection of all factors supporting and restricting the operation of components.

Definition 3.5 (Composition of Component) Composition of component refers to the operation of integrating components into the environment of component.

Integrating components into the environment of component means to compose a program with many components. Once the component is composed, it becomes a part of the environment of components. Before the component is composed, it is interrelate to and different with the environment of component. The component takes the environment of component as external environment for its existence and evolution.

Definition 3.6 (Behavior of Component) Behavior of component refers to the process of changing the states of the environment of component due to the implementation of components. The result of changing on the environment of component is called the results of component behavior.

If installing a program on a computer, the result obtained after running it doesn't come from the program, but from the computer system. That is to say, installing program is to integrate the program into the computer system and the program adds additional function to the computer system. The composition of component is essentially the same.

Definition 3.7 (Self-contained concept component set) It is assumed that C is an operator for component composition, Select is a selector of component, Proc can be any program and cCS is a concept component set according to definition 3.2.

If

$$Proc \equiv \mathop{C}_{i=1}^{m}(Select(cC_j)),\ \ (cC_j \in cCS) \wedge (j = 1-N) \wedge (1 < m < \infty) \qquad (3.1)$$

Then cCS is self-contained concept component set.

In general, concept component not only has limited behaviors and appropriate granularity, but also can implement specified sub-business logic through composition.

3.2 Domain Component

Domain component (dC) can be regarded as concept component limited by the application characteristics of a domain. Comparing with concept component, there are more restrictions on domain component. According to the characteristics of application in domain, domain component could be classified into two categories, one is general component (e.g. mathematic function, GUI, GIS, etc.) and the other is special component (e.g. computation of average precipitation, runoff generation and conflux computation, etc.), which is

$$dC ::= general\text{-}component \mid special\text{-}componen$$

Special component is either a framework component (application framework of domain) representing the relationship between sub-business logics or non-framework component representing the sub-business logics, which is

$$special\text{-}component ::= component \mid framework$$

The major difference between application framework and special component is that special component represents sub-business logic while the application framework represents the relationship between sub-business logics or relationship between components. The framework that represents a business applying all the relationship between sub-business logics is called main framework. Domain components can include general components.

Definition 3.8 (Self-contained domain component set) It is assumed that DA (Domain Application) is a program in domain D, dCS(domain component set) is a numerable set, $|dCS| = N,\ 0 < N < \infty$, domain component $dC \in dCS$, C is an operator for component composition, and Select is a selector of component.
If

$$DA \equiv \mathop{C}_{i=1}^{m}(Select(dC_j)),\ \ (j = 1-N) \wedge (m > 0) \qquad (3.2)$$

Then dCS is the self-contained domain component set of D.
Comparing formula (3.1) and (3.2), it shows that the difference between domain component set and concept component set are:

(i) Domain component set doesn't requires no relationship between each element, that is to say, pre-composed component with large granularity (composite component) is allowable in the domain component set;
(ii) Domain application program (DA) can be comprised with only one component;
(iii) Self-contained domain component set is a subset of self-contained concept component set's power set, which is $dCS \subseteq P(cCS)$.

Definition 3.9 (flexibility of component) Flexibility of component refers to the consistent results of component's behavior in various environment of component.

Flexibility can reflect the adaptability of component to different component environment. If a component can be integrated into different environment of component and obtain consistent result of behavior, this component has better flexibility. The composition of flexible component is called flexible composition.

4. MECHANISMS OF FLEXIBLE COMPOSITION

The mechanism of flexible composition of domain components is a combination of basic concepts, methods and relationship between interrelated factors of flexible composition of domain components, including flexibility of component, flexibility control and correlation between component and the environment of component.

4.1 The Basis of Flexible Composition of Domain Component

To suppose the domain program Proc is a finite-state automata

$$Ms = <Qc, \Sigma, \Gamma, \delta s, \lambda s>$$

among which Qs is a finite state set,
Σ is a finite input set,
Γ is a finite output set,
δs: Qs×Σ→Qs is a function for state transformation and
λs: Qs×Σ→Γ is an output function.
If there is another finite-state automata:

$$Mc = <Qc, \Sigma, \Gamma, \delta c, \lambda c>,$$

among which Qc is a finite state set,
the definitions of Σ and Γ are the same with those in the Ms,
δc: Qc×Σ→Qc is a function for state transformation, and
λc: Qc×Σ→Γ is an output function.
and

$$Qc \subseteq Qs;\ \delta c = \delta s \uparrow (Qc \times \Sigma);\ \lambda c = \lambda s \uparrow (Qc \times \Sigma)$$

(↑ refers to constraint),
then Mc≤Ms, which means Mc represents the component of program Proc. Namely the component can be composed to Proc. Obviously, Mc is equivalent to Ms if Qc = Qs.
The analysis shows that

(i) The component of program can be described with the sub-automata of finite-state automata;
(ii) The granularity of component is equal to |{δc}|+|{λc}|.
(iii) If Qc = Qs, then the component is program itself.

(iv) $\{\delta c\} \cup \{\lambda c\}$ is the behavior of component.
(v) Supposing $Q \in Qc$ is the initial state of Mc and $F \subseteq Qc$ is the final state set of Mc, then $\{Q\} \cup F$ represents the state interfaces of component and F is the result of component's behavior. Furthermore, the recognizable language set of Mc defines the data interfaces DI, which is $\{DI\} \subseteq \Sigma^*$.
(vi) Change of any factors including Σ, Γ, δc, λc, Q and F will result in changes on component's behavior. If the behavior of a component is adjustable, the data interfaces or state interfaces of component must be configurable unless the source code is changed.

In Mc, $Q \in Qs \wedge F \subseteq Qs$. If Proc is composed with several components, there must be several Qs, Fs and DIs. The precondition of composition is to define the relationship of Q and F with DI.

Definition 4.1 (Domain Application Framework, DAF) Domain application framework refers to the relationship between each component that composing the application of domain.

Supposing that {Q, F} is the initial state set and final state set of all Mcs that compose Proc. {DI} is the corresponding data interface set, then DAF is the relationship of $\{Q,F\} \times \{Q,F\} \times \{DI\}$. The form of DAF depends on the requirements of business logic and reflects process control of component's operation.

4.2 Flexible Composition and the Environment of Component

Definition 4.2 (Flexible Composition) Supposing that DA is any application in specific domain D; domain component set dCS is a numerable set ($|dCS| = N,\ 0 < N < \infty$); domain components $dC \in dCS$ and can be used to flexible composition; C is an operator for component composition; Select is a component selector; and F_config is an operator for flexible configuration of component, then the flexible composition of component can be expressed as:

$$DA \equiv \underset{i=1}{\overset{m}{C}}(F\_config(Select(dC_j))),\quad (j = 1-N) \wedge (m > 1) \wedge (dC_1 \in \{DAF\}) \qquad (4.1)$$

In special domain, due to application framework and flexible composition of dC, dCS may not be a self-contained domain component set in domain D and not all of dCs possess the characteristics of flexible composition.

Since components implement sub-business logic and framework implements the relationship between sub-business logics, following rules should be followed for flexible composition of domain components:

(i) Components can only be composed with framework.;
(ii) Framework can include frameworks;
(iii) The framework that can represent all the relationships between the components within whole business logic is called main framework, the main framework has relativity;
(iv) The flexible composition of component can be supported by framework and non-framework component that can be composed flexibly. However, not all frameworks and components need flexible composition.
(v) Once the composition is completed, it can not follow the mechanism of flexible composition to directly adjust the behavior of components.

A business application should contain at least one framework (main framework) that can represent all the relationship between sub-business logics. The main framework implements the business logics by connecting various components and frameworks. In regard to the composition of components, main framework can also represent operation environment of components. As an entity that is composed firstly, main framework can integrate other components, that is to say, main framework plays the role of "container".

According to definition 3.4, the environment of component is consisted of the operation environment of components and business logics that the component is adapted to. Operation environment of components is the operation platform of components, including required hardware, operating system, network platform, host language, application schema and type of database. The business logics that component is adapted to, is a description of the condition for component implementing behavior. The environment of component is the basic support and constraint for the implementation and evolvement of component behavior, which can be changed with the composition of component. Once component is integrated into component environment, it will immediately become a part of the environment of component and influence following composition. The environment of component is a combination of all the above-mentioned factors.

4.3 Classification of Flexibility of Component

In order to realize flexible composition, the components should be adapted to each elements of the environment of components, in another words, it has to ensure that component can match with corresponding element value of the environment of component by means of configuration.
Hardware and operating system are the foundation of operating domain applications. The capability of component in adapting to different hardware and operating systems is called flexibility on basic platform.

The flexibility of component reflected on network environment mainly refers to its adaptability to different network protocols, interoperation protocols, bandwidth and security control, which is call flexibility on network.

The adaptability of component to the operation environment of different host languages is called flexibility on language runtime.

Different application schema will have different requirements for components. If component can work under different application schema, it is called flexibility on application schema.

If component can identify data from different types of database and operate correctly, it is called flexibility on database. Obviously, the component that doesn't operate database doesn't require this kind of flexibility.

If component is capable of adapting to changes of business logics, in another words, the behavior of component can be changed through external configuration, the component has flexibility on behavior, which means the functions of component is configurable. This is adaptive to the requirement of application.

Within a practical application system of domain, the environment of components mainly includes two parts: one is the operation environment and requirements of business logic.

The requirement on the flexibility by the former part is a problem so called "cross-platform", which is based on technologies including software transplant, virtual machines and distributed object interoperation technology. While the requirement on flexibility by the latter part is to adapt to the difference of business logic, which is a problem so called "cross-application" and requires to resolve static configuration and dynamic adjustment of component's behavior. Therefore, the flexibility of component on operation supporting environment is called flexibility on platform, while the flexibility of business logics is called flexibility on behavior.
If a component has any kind of flexibility, the flexibility should not only be realized during programming but also be described correctly so that flexible composition of such component can be implemented. Formalized description is the appropriate method to ensure correct description. For more convenient applying in domain, it can establish relevant technical standards in domain to simplify description and computing methods of flexible composition.

Hereby, the core of flexible composition of domain components is how to match the elements of environment to which the components can adapt with the corresponding elements of environment which the components are integrated into.

5. CONCLUSIONS

This paper conducts a fundamental research on flexible composition of domain components, aiming at providing basic technical system for applying component technology in specific domain.

Based on previous researches on composition of components, this paper discussed the application of component technology in specific domain. Through explaining concept component and composition of components as well as defining some basic concepts including domain component, framework, behavior, granularity, self-contain component set, environment of component and classification of flexibility, following conclusions can be drawn:

(i) Composition of domain components is to integrate components into the environment of component;
(ii) Behavior of component is a process of changing the state of the environment of component due to the implementation of component.
(iii) Flexible composition is based on the component's capability of flexible composition.
(iv) The flexibility of component means data and control interface of component are configurable.
(v) The flexibility of component can be classified into two categories, flexibility on platform and flexibility on behavior. The former refers to "cross-platform" problem existing in domain application while the latter refers to "cross-application" problem.
(vi) In specific domain, it can reduce the difficulty of flexible composition of components by standardizing the description for elements of component's environment.
(vii) Domain application framework is an important factor for implementing flexible composition of domain components.
(viii) The three basic characteristics of component – encapsulation, reusability and composition, are important theoretic support for research on flexible composition of domain component.

REFERENCES

[1] McIlroy M D. Mass-Produced Software Components, "Software Engineering Concepts and Techniques"[A]. In: *1968 NATO Conference on Software Engineering*[C]. Van Nostrand Reinhold, 1976, pp.88-98.

[2] Guijun Wang, Liz Ungar, Dan Klawitter. "Component Assembly for OO Distributed Systems" [J]. *IEEE Computer*, 1999, 32(7):71-78.

[3] Fabio Kon, Roy H. Campbell. "Dependence Management in Component-Based Distributed Systems" [J], *IEEE Concurrency*, 2000, 8(1): 26-36.

[4] A.P. Barros, A.H.M. ter Hofstede, C. Szyperski. "Retrofitting workflows for B2B component assembly" [C]. *Proceedings of the 25th Annual International Computer Software and Applications Conference (COMPSAC'01)*, IEEE Computer Society, 2001.123-128.

[5] John Penix. "Deductive Synthesis of Event-Based Software Architectures" [C].*14th IEEE International Conference on Automated Software Engineering*, Cocoa Beach, Florida, USA, 12-15 October, IEEE, 1999.

[6] Bridget Spitznagel, David Garlan. "A Compositional Approach for Constructing Connectors" [C]. *Proceedings of the Working IEEE/IFIP Conference on Software Architecture (WICSA'01)*, IEEE Computer Society, 2001. 148-157.

[7] Zhong Wang, Zhongxian Chi, Chen-guang Wang. "MAC: a Component Reuse Architecture Based on Multi-agent Adapter" [C]. *Proceedings of the 14th IEEE International Conference on Automated Software Engineering* ,Cocoa Beach, Florida, USA,IEEE, 12-15 October, 1999.

[8] Uwe Abmann, Thomas Genbler, Holger Bar. "Meta-programming grey-box connectors" [C]. *Proceedings of the Technology of Object-Oriented Languages and Systems (TOOLS-33'00)*, IEEE,St. Malo, France , 5-8 June 2000.300-311.

[9] XU Jia-fu, LU Jian. *The Software Language and Its Implementation* [M]. Beijing: Science Publishing Company, 2000.

Ping Ai is a Ph.D. and a full professor, senior member of china computer federation (CCF) and member of IEEE, chief professor of the State Key Laboratory of Hydrology-Water Resources and Hydraulic Engineering (Hohai University) of China. He has undertaken several research projects supported by the National High-Tech Research and Development Plan of China; the National Grand Fundamental Research 973 Program of China; the Foundation of Nature Science and Hi-Technology of Jiangsu Province of China; the Key Project of Science and Technology Research of the Ministry of Education of China, the Foundation of Science and Technology of the Ministry of Water Resources of China, and he has published a book, over 30 papers in the journals and the international conference proceedings. His research interests are in architecture of computer application system in specific domain, software component and Web component, intelligent data processing and knowledge application system.

Software Architecture for Adaptive Distributed Multimedia Systems*

Guiyun Ye[1], Changzheng Liu[2]
[1]College of Electrical and Information Engineering, Heilongjiang Institute of Science and Technology
Harbin, Hei Longjiang, 150027, P.R.China
[2]College of Computer Science and Technology, Harbin University of Science and Technology
Harbin, Hei Longjiang, 150080, P.R.China
[1]Email: yeguiyun@yahoo.com.cn [2] Email: fox@hrbust.edu.cn

ABSTRACT

To support multimedia applications in mobile environments, it will be necessary for applications to be aware of the underlying network conditions and also to be able to adapt their behaviour and that of the underlying platform. This paper focuses on the role of middleware in supporting such adaptation. In particular, we investigate the role of open implementation and reflection in the design of middleware platforms such as CORBA. The paper initially extends CORBA with the concept of explicit binding, where path of communication between objects is represented as first class objects. We then introduce the concept of open bindings which support inspection and adaptation of the path of communications. An implementation of open bindings for adaptive continuous-media interaction is described using the example of adaptive video-on-demand for mobile environments.

Keywords: Mobile Environment, Middleware Platform, and Open Binding, Adaptive Video-on-Demand

1. INTRODUCTION

Future computer systems will consist of end-systems which will be disconnected, weakly connected by low speed wireless networks such as GSM, or fully connected by fixed networks ranging from Ethernet to ATM. Furthermore, the level of connectivity will vary over time as a consequence of the mobility of the modern computer user. Even when connected to a particular network, fluctuations in throughput and delay may be experienced due to congestion (e.g. as witnessed in the Internet).

To cope with such variations, it is important that systems can adapt to the quality of service offered by the network. Such adaptation can take place at a variety of levels in the system, in the operating system or in the application. In this paper, we are concerned with support for adaptation in the middleware platform (i.e. the layer of software above the operating system), which offers a platform independent programming model and hides problems of heterogeneity and distribution. More specifically, we consider the design of middleware plat-forms which (i) allow the application to inspect the current level of QOS at various points of the system, and (ii) enable applications to dynamically adapt their behavior or the behavior of the underlying platform in response to changes in QOS. We are particularly interested in adaptation as required by multimedia applications.

A range of middleware technologies is now available, including CORBA, DCE, and DCOM. In addition, ISO have recently completed an international standard defining a reference model for open distributed processing (RM-ODP); this standard provides a framework for the development of middleware platforms. In this paper, we focus on the CORBA platform from OMG, although many of the arguments could be applied to other platforms. CORBA provides an environment whereby objects can interact in a distributed environment. Objects are defined in a language and platform independent manner through an interface definition language (IDL). An object request broker enables clients to issue requests on an object; the ORB locates the object, transmits the request, prepares the object implementation for receiving and processing the request, and conveys results back to the client. (Further details of CORBA can be found in [3].)

A major problem with CORBA is that, until recently, the architecture has adopted a traditional black box approach whereby the implementation of the platform is hidden from the application. Recent work in the OMG forum [31, 33] has started to alleviate this problem; however few CORBA implementations have taken these ideas on board. Traditionally, the 'black box' nature of CORBA has not been a great problem. It could be argued that this is a highly desirable property of a middleware platform. With the advent of mobile (multimedia) computing, however, such an approach is untenable; in such environments, it is essential to have (selective) access to the underlying implementation. To achieve this, we adopt concepts from open implementation [20] and reflection [23]. In this paper, we focus on the use of such techniques to enable inspection and adaptation of the path of communication between interacting objects. In other research at Lancaster, we also consider the use of such techniques in other aspects of a middleware platform (e.g. concurrency control, thread scheduling and real-time synchronization) [4].

2. OPEN IMPLEMENTATION AND REFLECTION

The concept of open implementations has recently been investigated by a number of researchers, most notably Kickable et al. at Xerox PARC [20]. The goal of this work is to overcome the limitations of the black box approach to software engineering and to open up key aspects of the implementation to the application. This must, however, be achieved in such a way that there should be a principled division between the functional-ity they provide and the underlying implementation. The former can be thought of as the base interface of a module and the latter as a meta-interface [34].

The role of reflection is then to provide a principled means of achieving open implementation. In a reflective system, the meta-level interface provides operations to manipulate a causally connected self-representation of the underlying implementation. According to Maes [23], a system is said to be

* This work is supported by the Natural Sciences Foundation of Heilongjiang Province under Grant QC04C44, Doctor Foundation mgb05006, Natural Sciences Foundation of China mgz06011 and the Foundation of office of Education of Heilongjiang Province under Grant 11511070.

causally connected to its domain if 'the internal structures and the domain they represent are linked in such a way that if one of them changes, this leads to a corresponding effect on the other'. Such a system has the benefits that, first, the self representation always provides an accurate representation of the system, and that, second, a reflective system can bring modifications or extensions to itself by virtue of its own computation. In other words, a reflective system naturally supports inspection, and adaptation.

2.1. Inspection
Through reflection, applications are able to observe the occurrence of arbitrary events in the underlying implementation. Such an approach can be used to implement functions such as QOS monitors or accounting systems in a portable manner.

2.2. Adaptation
Similarly, reflection allows applications to adapt the internal behavior of the system either by changing the behavior of an existing service (e.g. tuning the implementation of message passing to operate more optimally over a wireless link), or dynamically reconfiguring the system (e.g. inserting a filter object to reduce the bandwidth requirements of a communications stream). Such steps are often the result of changes detected during inspection (see above).

Most of the early research in reflection focused on the field of programming language design [20, 38]. More recently, the work has diversified with applications of reflection in areas such as windowing systems [34] and operating systems [39]. There is also growing interest in the use of reflection in distributed systems. Pioneering work in this area was carried out by MacAfee [25]. More recently, researchers at APM have developed reflective extensions to Java with a view to supporting distributed applications. However, there has been much less activity to date in the design of reflective middleware. Campbell at Illinois has carried out initial experiments on reflection in object request brokers (ORBs) [36]. The level of reflection, however, is coarse-grained and restricted to invocation, marshalling and dispatching. In addition, the work does not consider key areas such as support continuous media interaction. Manola has carried out work in the design of a 'RISC' object model for distributed computing [24] (i.e. a minimal object model which can be specialized through reflection). A PhD student of Cointe is also investigating the use of reflection in proxy mechanisms for ORBs [21].

3. INTRODUCING EXPLICIT BINDINGS

To address our requirements, it is necessary to extend the programming model offered by CORBA [3] (thereby aligning it more with ISO RM-ODP). In particular, we introduce the concept of explicit binding. In the current CORBA programming model, binding is implicit in that, when objects interact, an appropriate communications path is created by the underlying ORB. In fact, it is worth noting that the term binding is used here as it is in the ISO RM-ODP model to refer to the end-to-end mechanisms at all levels which enable distributed interaction between objects; in contrast the CORBA usage refers to several concepts including that by which an object implementation is found for a given object reference [15].

In this paper, we are particularly interested in this second aspect of explicit bindings (i.e. support for inspection and adaptation).

We introduce two different styles of binding, namely operational bindings and stream bindings: operational bindings support the traditional style of interaction in CORBA, namely operation requests. Stream bindings are then required to support continuous media interaction. A given stream consists of one or more flows where each flow represents the unidirectional transmission of a continuous media type (e.g. audio or video). As a result of this change, it is also necessary to distinguish between operational interfaces and stream interfaces as end-points of operational bindings and stream bindings, respectively.

The architecture is open in that bindings are created by an extensible set of binding factories. Factories in CORBA are objects that support the creation of a particular class of object; binding factories are therefore responsible for creating a new binding between a target set of objects. One binding factory could provide the semantics of standard CORBA requests whereas another could provide real-time guarantees in terms of end-to-end latency (perhaps exploiting meta-level functionality to meet the required guarantees). Similarly, for continuous media interactions, one factory could provide a best effort service for video transmission, whereas another factory could provide guarantees through an appropriate resource reservation strategy. In addition, programmers are free to develop their own binding classes, perhaps in terms of existing classes. Explicit bindings provide one step towards a more open architecture in that communication becomes both visible and controllable. This is necessary but, in our view, not sufficient for mobile multimedia applications. We therefore extend this concept further by introducing open bindings.

4. CONCEPT OF OPEN BINDINGS

4.1 General Approach
To support mobile computing, it is necessary for the application to be able to exert some control over bindings. One way of achieving this is for binding interface to offer QOS management operations to monitor the current levels of QOS and to adapt to perceived changes. The problem with this approach is that it is very difficult to design a general means of achieving adaptation. This is especially problematic when mobility is introduced, owing to the proliferation in possible actions. Our approach is for bindings to offer a meta-interface providing access to a causally connected self-representation. This self-representation is provided by an object graph, representing the underlying end-to-end communications path. This equates to a procedural as opposed to a declarative approach to QOS management [2]. We argue that this approach offers the level of flexibility required by mobile computing. This procedural approach is influenced by our experiences with the use of logic or QOS attributes to specify QOS requirements [7]. We have found that this is a perfectly valid approach for dealing with static QOS properties, but the approach cannot easily be extended to deal with adaptation. In Adapt, we still allow the association of some simple QOS attributes defining media types with bindings as a means of checking consistency between interfaces in the bindings. However, the main mechanism for dealing with more dynamic aspects of QOS management is to directly manipulate graphs.

Note that this does not preclude the use of declarative techniques which can be built on top of the basic procedural facilities provided by the platform.

4.2 Object Graphs

An object graph consists of processing objects and binding objects which are connected together by local bindings. Communication across a local binding is assumed to be instantaneous and reliable, normally implying that local bindings are located in a single address space or a single machine. All other interactions are represented explicitly by the binding objects in the graph. Processing objects then either perform computations on the data flowing through the graph or are responsible for a particular management function. Examples of processing objects include QOS filters and mixers, QOS monitors, or rate control components.

To control visibility of interfaces within a binding, we introduce the concept of interface mapping. Interface mapping allows an external interface to map on to the interface of an internal component. The external interface acts as a proxy for the internal interface; all interactions occur at the internal interface via the external interface.

As a further refinement, binding objects can them-selves be open bindings and hence also be composed in terms of object graphs. The nesting bottoms out by offering a set of primitive bindings whose implementation is closed. For example, a particular platform might offer RTP or IP services as primitive bindings (depend-ing on the level of openness in the platform). This nested structure provides access to lower levels of the implementation (if required). At a finer granularity, each object in the graph can offer an interface to con-trol its individual behavior.

4.3 Type Checking in Object Graphs

To ensure a basic level of consistency in object graphs, strict type checking is mandatory for all local bindings. When a local binding is requested between two inter-faces, a media type must be found which is acceptable to both, otherwise the local binding cannot proceed. This process of media type negotiation requires information on the media type(s) that each interface can produce or consume.

Other researchers have investigated the extending of IDL to include media type description as part of an interface definition [3]. However this introduces inter-ORB compatibility problems by modifying an accepted standard, OMG IDL. Moreover, this approach is unsuited to the highly dynamic adaptive application areas investigated in the Adapt project. Rather than extend IDL, we instead augment stream interfaces with operations allowing their accepted media types to be queried dynamically. This alleviates the need to have access to compiled interface definitions.

5. USING OPEN BINDINGS

5.1 Component Class

In our current C++ implementation, every object descends from the Component class. This class pro-vides the basic functionality required by extending the basic CORBA object class in several different ways.

(1) First the Component class enables objects to export multiple interfaces, both stream and operational, using a mechanism similar to that used in Microsoft's COM/ DCOM. This allows objects to possess multiple stream interfaces thus creating the basis for multimedia processing and interaction.
(2) Secondly, using this multiple interface support, the Component class exports a meta-interface, Metacomponent. This interface provides access for inspection and adaptation to the component's implementation object graph.
(3) Thirdly, the Component class provides the initial support for 'plug and play' semantics by providing methods to query the number and type of stream inter-faces associated with a component; and also to ascertain whether or not a particular stream interface will accept a local binding.
(4) Finally, the Component class introduces an event mechanism allowing interested parties to register for particular events, delivered by way of a callback.

One use of this is to enable monitoring components to pro-duce events in response to QOS fluctuations. These events can then be acted upon by management components, such as the reactive objects investigated in earlier research at Lancaster [3]. Monitoring components themselves are a well-defined way of interfacing to particular QOS monitoring systems. For example, the protocol layers being developed for the Ensemble protocol suite as part of the Adapt project [8].

5.2 MetaComponent Class

The MetaComponent interface class exists to make the object graph of a component available for inspection and adaptation. This is achieved primarily by the use of a graph data structure, which describes each object in the graph, and the interconnections between them. This data structure allows the programmer to traverse the graph to examine the way in which the component it represents is implemented. Using the example in Section 5, one could ascertain that the binding object used MPEG compression objects interconnected by a trans-port binding object, but that no jitter-compensation component was used.

This level of information allows more educated decisions on how adaptation mechanisms are to be applied. An example in this case would be the insertion of the jitter-compensation buffer component triggered by events from a network monitoring component indicating that the level of jitter on the net-work had increased. Section 5.3 examines how the meta-interface of a component such as a binding object can be used to provide support for adaptation in this manner.

Apart from providing inspection and change access to a component's implementation, a MetaComponent interface is also responsible for policing this access to maintain consistency and security. This is aided by the indirect identification of implementation components in an object graph. Rather than use their CORBA interface references, opaque unique identifiers are used instead. The actual interface reference must be requested from the meta-interface. The particular instance of meta-interface may choose to make all components visible, or perhaps to restrict access to only certain 'safe' implementation components. Once an interface reference has been made public, there is no way (in standard CORBA) to police invocations on this object, and therefore consistency may be compromised.

5.3 Adaptation with Open Bindings

This is the simplest form of adaptation. To modify the behavior of a component, the application must first obtain the interface for this component via the graph traversal as described above. Once the application has obtained this interface, the programmer can make changes to that component such as increasing the delay length of the buffering component or altering the compression strategy of the MPEG component. The precise interface is clearly dependent on the object class of the component, although interface inheritance is used extensively to create a large hierarchy with many 'base' interfaces, thus allowing complex components to offer increasingly specialized interfaces. An example of this is a media filtering object that, at one level, implements a basic, abstract, Media Filter interface which offers a setQualityPercentage() method, while also defining a subclass of this interface which includes more specific operations dependent on the particular media type being filtered by that component. Polymorphism is used to allow basic controller components to manipulate other components without having to know of their specific inter-face type.

6. CONCLUSIONS

This paper has considered the design of middleware platforms to support mobile multimedia applications, and has explored the notion that middleware platforms should be adaptive in order to address the diverse requirements imposed by such applications. The paper has also outlined the design of an adaptive middleware platform, based on CORBA, but extended with the concepts of stream interfaces, open bindings and object graphs.

REFERENCES

[1] L. O. Chua, L. Yang, *Cellular neural networks: Theory*, IEEE Trans. Ciruits Syst.-I Vol.35, pp.1257-1272, 1988.

[2] L.O. Chua, L.Yang, *Cellular neural networks: Applications*, IEEE Trans. Circuits Syst.-I, Vol.35, pp.1273-1290, 1988

[3] T. Roska, L.O. Chua, "Cellular neural networks with nonli-near and delay-type template," *International Journal of Circuit Theory and Applications* Vol.20, pp.469-481, 1992.

[4] J.J. Hopfield. "Neural networks and physical systems with emergent collective computational abilities," *Proc Nat Acad Sci USA*, Vol. 79, pp.2554-2558, 1982.

[5] J.J. Hopfield. "Neurons with graded response have collective computational properties like those of two-state neurons," *Proc Nat Acad Sci USA*, Vol. 81, pp.3088-3092, 1984.

[6] Zhanji Gui, *Biological dynamic models and computer simulation*, Beijing: Science Press, 2005.

[7] Zhanji Gui and Weigao Ge, "Existence and uniqueness of periodic solutions of nonautonomous cellular neural networks with impulses," *Physics Letters A*, Vol. 254, pp.84-94, 2006.

[8] Zhanji Gui and Weigao Ge, "Periodic solution and chaotic strange attractor for shunting inhibitory cellular neural networks with impulses," *Chaos*, 16, 033116, pp.1-10, 2006.

[9] Zhanji Gui and Weigao Ge, "The effect of harvesting on a predator–prey system with stage structure," *Ecological Modelling*, Vol. 187, pp.329-340, 2005.

[10] Zhanji Gui and Weigao Ge, "Periodic solutions of nonautonomous cellular neural networks with impulses, Chaos," *Solitons & Fractals*, Vol.32, pp.1760–1771, 2007

[11] Zhanji Gui, Deming Yuan, "Stability of artificial neural networks with impulsive inputs from outside the network," *Journal of Computational Information Systems*, Vol.2, pp.1045-1050, 2006.

[12] Y. Li. "Global exponential stability of BAM neural networks with delays and impulses," *Chaos Solitons and Fractals*, Vol. 24, pp.279-285, 2005.

[13] V. Lakshmikantham, D.D. Bainov, P.S. Simeonov. "Theory of impulse differential equations," *World Scientific*, Singapore, 1989.

Guiyun Ye is a vice Professor of College of Electrical and Information Engineering, Heilongjiang Institute of Science and Technology. She graduated from Harbin Engineering University in 1986. She has published over 30 Journal papers. Her research interests are in distributed parallel processing, Visualization in Scientific Computing.

Changzheng Liu is a vice Professor of Computer Science and Technology College, Harbin University of Science and Technology. He graduated from Harbin Engineering University in 1993; was a postdoctor of Harbin Medical University (2004~2006). He is secretary-general of Hei Longjiang Biomedical Engineering Society. He has published over 20 Journal papers. His research interests are in distributed parallel processing, Visualization in Scientific Computing.

Technology on the Static Analysis of System Subject to Regression Test with Software Developed Based on the C, C++ Language

Yun Lei
College Of Computer And Information Engineering, Lishui University
Lishui, Zhejiang 323000,China
Email: **Leiyun11@163.com**

ABSTRACT

The technology of system syntax analysis was used in the regression test .And using C++Test, an automatically test driving system , it was done that lexical, syntax analysis and pretreatment of C,C++ source code, build the EFSM model, analysise the data dependence and control dependence, excute the test case to carry out regression test. The provement of veracity and correction ratio, and a decrease software period.

Keywords: Regression Test, Syntax Analysis , Dependence Analysis

Software testing serves as an important link of software engineering. With the expansion of software system, software testing has become an important means for the assurance of software quality. Regression test aims to guard against any side effect imposed by any alteration to the software on other parts of the software, so as to ensure the running of software to the altered target. Regression test plays an important role in the process of software testing. Following the wide application of extended finite state machine (EFSM) in modeling [1], extensive investigation has also been made into testing methods. C++Test prototyping system is a drive system for automation testing, of which, major functions include static analysis and preprocessing of C, C++ source program, generation of system finite automaton model, dependency analysis, regression test and generation of final test report. The public information database obtained through static analysis serves as the basis of C ++ Test system as well as the EFSM analysis and dependency analysis of the system[2,3,4].

1. STATIC ANALYSIS

1.1 Technologies on the Realization of Static Analysis

Module for lexical and grammatical static analysis mainly aims to analyze codes of C++ source program so as to extract major features of source program and obtain results of intermediate analysis to be input into the public information database. As the foundation of the system, these analysis results can provide necessary bases for the preprocessing of source program and automatic generation of driver.

As programs subject to testing must have been certified through the compilation, morphemic and grammatical error is unlikely in existence. Therefore, it is no need to check and process it.

Lexical analysis aims to mark off conventional C++ morphemes represented by such terminal characters as keywords, special symbols, annotations, ID and NUM for the purpose of facilitating the read-in for grammatical analysis. Lexical analysis constitutes an integral function, of which, any returned integral is the code (or the type of terminal character) of corresponding terminal character identified. As the return values are required to represent values of terminal characters in some cases, we can achieve this goal by endowing the YACC defined global variable yylval with the said return values. The task of lexical analysis is to perform semantic analysis of the results of lexical analysis, so as to verify if there is any grammatical error, and provide guidance for follow-up analysis and processing. As the focus of testing lies in the logic control structure of the program, detail information represented by arithmetic expression and assignment statement, which are not related to logic control structure can be well dispensed with when performing the lexical analysis. Through manual compilation of semantic action, the lexical analysis makes use of the YACC to generate corresponding source files, including C++ library function, global variable chart, keyword list, all combined definitions, terminal characters and type description, nonterminal characters as well as various functions for semantic action and lexical analysis as required by grammar regulations and syntax rules.

Lexical analyzer of the system is generated by its generator, LEX; whereas, grammatical analyzer is generated by its generator, YACC. This approach is helpful in minimizing the unnecessary manual labor, ensuring the appropriate structure of public information database and laying emphasis on the compilation of semantic subprogram. It can also facilitate the maintenance of programs for lexical and grammatical analysis programs.

1.2 LEX, Lexical Analyzer Generator

In 1972, M.E.Lesk and E. Schmidt from Bell Laboratory developed for the first time, LEX, the so-called lexical analyzer generator based on the Unix operating system. After that, LEX was launched in together with Unix system as its standard program. This system adopts the LEX analyzer attached to Parase Generator.

LEX file aims to mark off conventional C++ morphemes represented by such terminal characters as keywords, special symbols, annotations, ID and NUM by means of reading source program, so as to facilitate the input of grammatical analysis.

LEX file consists of three parts, namely program declaration, rules and program segment.

1.3 YACC, Grammatical Analyzer Generator

As same as the LEX, YACC is also a standard utility program (Utility) of UNIX system. Formal grammar for conventional program design languages mainly adopts the LALR (1) grammar, which serves as a subclass of context － free grammar. Grammatical analysis for most of program design languages normally adopts the LALR (1) analysis sheet. Furthermore, YACC of Parase Generator also takes the LALR (1) grammar ad the basis. Similar to LEX, it also aims to generate LALR (1) analysis sheet through the analysis of input rules on formal grammar, so as to output C++ language source program for grammatical analyzer driven by the same analysis

sheet. The input file of YACC is also called YACC source file, which consists of a group of formal grammar rules written in Backus Naur Form (BNF) and C++ language statement used to the semantic processing of each rule. Function yyparse() output by the YACC for grammatical analysis makes of the function yylex() output by the LEX for lexical analysis to acquire code for current word. The interaction between lexical analyzer and grammatical analyzer will eventually complete the analysis of C++ source program file. The task of grammatical analysis is to analyze the results of lexical analysis, so as to verify if there is any grammatical error, and provide guidance for follow-up analysis and processing. As the focus of testing lies in the logic control structure of the program, detail information represented by arithmetic expression and assignment statement, which are not related to logic control structure can be well dispensed with when performing the lexical analysis. Through manual compilation of semantic action, the lexical analysis makes use of the YACC to generate corresponding source files, including C++ library function, global variable chart, keyword list, all combined definitions, terminal characters and type description, nonterminal characters and various functions for semantic action and lexical analysis as required by grammar regulations and syntax rules.

Grammatical analysis is a process of identifying the program structure, which aims to provide guidance for automatic instrumentation and automatic generation of test driver. The approach to realize the recursion drop is to write each item of syntax rules into a handler function, and take the previous function to determine the current status and make adjustments to relevant approaches for function processing.

1.4 Structure of Major Datum for Static Analysis

Public information database serves as the hub for contact system tools as well as the basis for the establishment of EFSM model and dependency analysis[5,6]. The system aims to input all necessary information into the public information database through the analysis and processing of source program. Any information as required by each tool can be selected from the public information database. On this account, the design quality of public information database has a direct influence on performance of the whole system. We have taken into full consideration various data stream / control flow information, dependent information, call information as well as other information on relation between each program entity. According to the demands of the whole system, we have also designed a public information database of perfect expandability and high access efficiency, which is capable of ensuring the uniform and accessible information. Public information database of this system is composed of several forms as represented by syntax tree, code list, variable declaration sheet, variable reference list, function list and function reference list.

1.5. Structure of Information Database

The system takes the syntax tree as the structural core for the purpose of reflecting interrelations between each function, type, variable and constant of the program as well as the scope structure and the text structure of the program. Furthermore, description of entity attribute of the program is incorporated into the information list, in an attempt to reflect the detail information on the entity with the adoption of different forms of structural description for different entities. This has laid a solid foundation for the establishment of EFSM and the dependency analysis in the future.

2. REALIZATION OF DEPENDENCY ANALYSIS

Once the EFSM modelis established, it is applicable to obtain each dependent relation through the analysis of EFSM control flow and data stream. This section aims to discuss on approaches as required for acquiring these dependent relations. The basic conception is represented by the preferential traversing algorithm of graphic depth[7,8].

Detailed algorithm procedures are stated as follows:

```
Start EFSM Dependence (t,v)
Input EFSM model
Output dependency graph of the EFSM system
1 begin
2     mark t “visited”;     //mark the initial set value of status transfer t as “visited”.
3     for each transition u of tail(t) do    //determine the preset status of t.
4     if u is marked “unvisited” then //if the status is marked “uninvited”,
5     if v ∈ def(u) then    // Variable v not defined yet.
6     begin
7     if v ∈ c-use(u) and v ∉ p-use(u) then
8     add v to T(t, z)
9     else
10          begin
11          if v ∈ p-use(u) then
12          mark u “data dependent” in T(t, z); //data dependency
13          if v ∈ c-use(u) then
14          mark u “control dependent” in T(t, z);//control dependency
15          end
16          EFSM Dependence (u,x)//recursion call
17          end
18 end;
```

The dependency graph of EFSM system can be obtained from the foregoing algorithm. As the dependency subgraph is adopted in the regression test, we can make use of the optional algorithm for regression test cases to acquire reversely, the dependency subgraph of the system, so as to determine the incidence of regression test.

3. REALIZATION OF REGRESSION TEST

Once the dependency subgraph of the EFSM system is obtained, we can start the regression test. The major problem with the regression test lies in the incidence of modification which can be determined with the help of dependency subgraph.

Detailed algorithm procedures are stated as follows:

```
Start Reg Test Select(D，TS)
Input coverage dependency set D, and test case set TS.
Output regression test case set TS‘
1 begin
2     while D ≠ ∅     //prerequisite for cycle is that the coverage dependency set shall not be left empty.
3     begin
4     for each testcase tc in TS do    //precedence ordering for all test cases
5     sort(tc,D) //Cover the D status transfer sorting as per test case.
```

```
6       push(tc, TS‘)    // Incorporate test cases covering
        most of status transfers into regression test case set
        after sorting.
7       D = D － {tc} //reset D
8       TS ＝ TS － {tc1} //Reset TS
9       end
10 end
```

Driven by our C++ Test system, the test case will be executed automatically. The test will come to a stop when it meets the coverage rule. Thus, the selected test case set can be obtained.

4. USER INTERFACE

This system is provided with a standard, intuitive graphic user interface (GUI) based on the Multi-Document Interface (MDI) on the Window platform. This graphic user interface mainly includes source program, code list, EFSM model, dependency analysis, test case and testing results.

Once a source program is selected, the system interface shall be displayed as shown in figure 4.1. The source code of the program is indicated at top right corner.

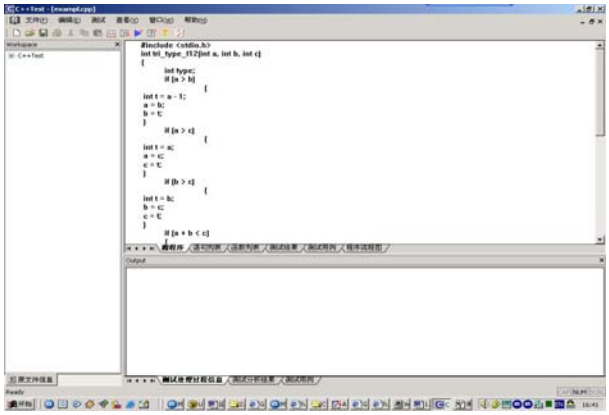


Fig4.1. The Opened Source Code

It is applicable to obtain code list, function list, variable list and so on by means of static analysis. Source program code list is as shown in the following figure.

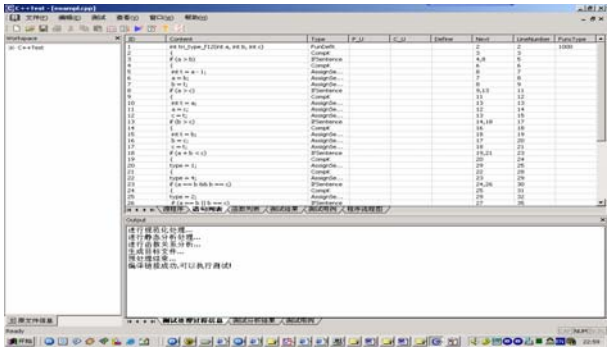


Fig 4.2 Program Code List

Once the static analysis is completed, perform the analysis of EFSM so as to obtain the EFSM model of the program. Shown in figure 4.3.

After the EFSM model is acquired, perform the dependency analysis to obtain dependency set before testing the drive probation case to obtain testing results.

5. CONCLUSIONS

The discussion on technologies on the realization static analysis as well as the data structure acquired for static analysis has laid a solid foundation for the establishment of EFSM and the dependency analysis, and has brought into being the visualized interface eventually.

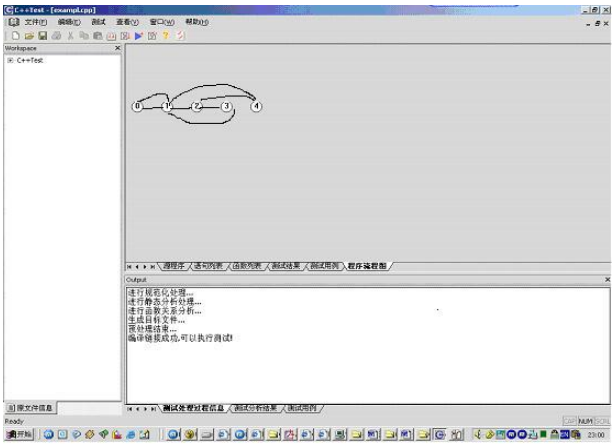


Fig 4.3 System EFSM Model

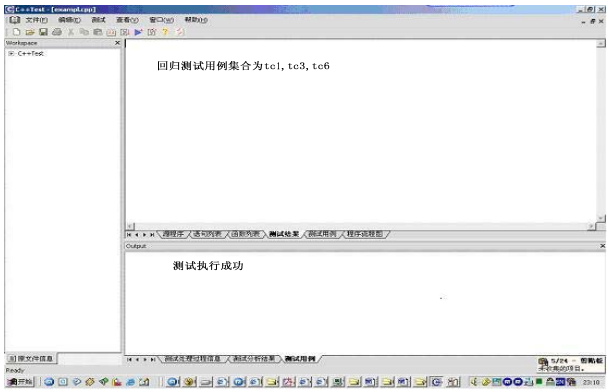


Fig 4.4 The Result of Regression Test

REFERENCES

[1] Zheng Renjie. Computer software test technology [M]. Beijing: Qinghua University publishing house, 1992. 5～38.

[2] G. Bochmann, V. Semantic Evaluation from Left to Right. Communications of the ACM ,1976 ,19(2) : 55～62.

[3] Jin Chengzhi. Compiler structure principle and realization technology [M]. Beijing: Higher education publishing house, 2000. 4～46

[4] Ma Rui-fang ,Wang Hui-ran. A Study of Computetr Software Testing Method[J]. Mini-micro Systems, 2003 24(12): 2210～2213

[5] Chen Aiguo. Software test and software reliability: [D].Preserves the place: Xidian University Library, 2001.

[6] Zhang Chun-xia,Su Qin. Analysis of Software Testing Process[J], Application Research of Computers, 2004, 05, 46~51

[7] Liu Jun, Liu Zhuojun .Upgrading & Using lex and yacc to Develop Message-Driven GUI Syntax Analyzing Software[J]. Computer Engineering And Design, 1999,

20(1), 72~75.
[8] Xiao Jun chao, Zhang Jia chen. Automatic Generation of LALR(1) Parser[J]. Computer Applications.2003, 23(04), 65～69.

First author: **Lei Yun**, the female, she race, the Zhejiang Lishui person, in January, 1981 lived, master graduate student, teaching assistant, specialized: The software engineering, mainly studies the direction: Database software and theory, computer software engineering.
Address: Zhejiang Province Lishui city Lishui institute computer and information engineering institute, zip code: 323000.

A Components Reuse Way Based on Fractal Theory Research*

Sen Yang, Qing Liu
Yunnan University
KunMing, Yunnan Province, China
Email: yang82101@163.com

ABSTRACT

This paper explained the components reuse way that based on fractal theory research. According to the thought of the catalyst method and the method of KobrA, thought of the self similarity process and the repeat characteristic of fractal to component developing process can be deduce by the mathematics theories for components reusing. Explained the component reusing and the theories how to constructs the database of component, then described the components software's software process and the component products by the mathematics of the self similarity. Hold from the essence of components reusing with mechanism.

Keywords: K-Component, Container-Tree, Fractal, Component- Dimension

1. INTRODUCTION

The developing methods which based to component provided the support on the technique for the Big-Degree-Components reusing. The method of KorbA [6] is a kind of face to the product wireman distance which can support the most extensive meaning of Component-Reusing, this method taking each one with abundant behavior as a K-Component ,this principle of the way of building model made a K-Component container tree had the characteristics of fractal. In another word, the process software engineer which faces to component and the product had the characteristic of self-similarity. It can lead a reusable developing process, while making the model which base to mathematics that described the way to how to organization a component database and how to inspect them.
As the fractal theories, the graphics working with repeating functions to build element to evolve into a fractal, the method of KorbA made the K-Component as the base graph evolve into the whole system as it in fractal, so we can use the fractal theories as the guide of component reusing.

2. BRIEF INTRODUCTION OF KROBA

2.1 The Characteristic of Three-Dimension

KorbA method divide the question of the software must resolve into three aspects [6]: Abstract degree, generality and synthesizability .Showing as Fig.1.
A software developing process begins at the top black box:

Erase the universal, make true specifications. If your paper deviates significantly from these specifications, the printer may not be able to include your paper in the Proceedings.

System which can meet the application need;

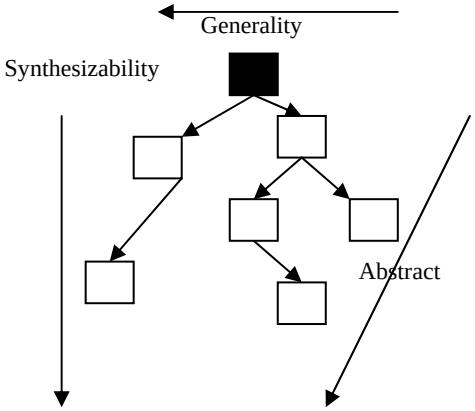


Fig.1. The generality and synthesizability

Dived the system into smaller degree to build up a Container-Tree for component nest;

Lower the Abstract degree to make each parts of the system close to application program

After these themes completed, the system which constituted by smart component with null universal or concrete can executable.

2.2 Container-Tree

All the processes of building the components system model can concentrating as a Container-Tree[6]. The base is a K-Component which contains all the components feather what the system need. By refinement on super K-Component, we can get the sub K-Component's specification.

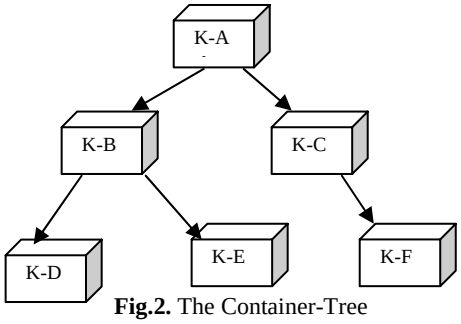


Fig.2. The Container-Tree

This Container-Tree has the characteristic of fractal because all the components are developing by unify principle. Every K-Component is developing by the same model needn't concern it place in this tree.
By this method, all the K-Components have the characteristic in the arbitrarily small mark degree (The fractal has the whole feature of gather),so the whole Container-Tree is a fractal.

2.3 The Same Form of Container-Tree and Synthesize-Tree

Opposite to the top-down-modeling, execute the system is a process of a bottom-up, small component synthesize large

* Support by YunNan University plans for the training of young and middle-aged teachers.
* Support by National natural science fund (2005~2007).

component.

The KrobA assurance the Container-Tree and Synthesize-Tree must consistent.

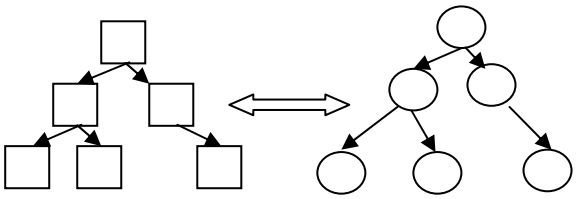


Fig.3. The Synthesize-Tree

In another word, component software has the same analyze and modeling process the developing and execute, so the last product is a system has the feature of fractal.

3. FRACTAL THEORY IN COMPONENT CONSTRUCTION

Turning a K-Component to a real one to construct a system is the essential step. A component which can exist in true software system can be developed by two ways:

Developing a new component to match the K-Component specification ;

Reuse a component which has been exist to match the K-Component specification;

The second way makes the software engineering working in High-efficiency, for example, though COTS can develop large software system by large-scale reusing.

3.1 The Component-Reusing Way in the KrobA Method

In the thinking of KorbA method, reuse a component is the process of fusion the extern component into current Container-Tree. This fusion way must assurance the Container-Tree has consistency.

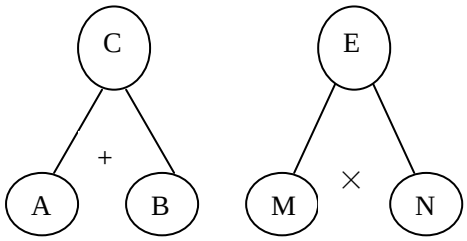
There are two type of component can be reused:
KorbA component, these component developed by KorbA method, but isn't a part in current Container-Tree
Different type component-Didn't developed by KorbA method, so it doesn't match K-Component specification.

We generate a K-Component by reusing extern component, component operation and matching-mapping is the usually way.

3.2 Component Operation

As thesis [2] notes, the relationship among components can be seen as operations. For example, "+" can describe two components work in corporation. "×" an describe two components work in erupting.

If container-tree has semantic, a K-Component is the result of two Sub-components makes operation:



C:=A+B E:=M×N

Fig.4. The Component Operation

Component operation can allocate, wedge bonding and exchange, so it is
possible to simulate multiple operation by these rules.
Now we use "*" to represent all kinds of operation, if n components
(c[1]~c[n])construct a new K-Component, We can change into the nether form with this form:

$$K = \prod_{i=1}^{n} Ci^{Hi} \qquad (1)$$

The value of 'H' can get all kinds of operation. If 'H' represents the value of edge, component as the note, this system change into a fractal (Neglect the dissimilarity of edge value), now container-tree is the data-strut of this fractal graph.

3.3 Matching-Mapping

If **k= Γ (c)** is a mapping that can change different type component(C) into k(k matching K-Component specification), **k= Γ (c)** (2) called Matching-Mapping.

When we make several components into a K-Component, according to (1) and (2), we can get the following formula:

$$K = \Gamma(\prod_{i=1}^{n} Ci^{Hi}) \qquad (3)$$

This formula called an adapter to a K-Component. The characteristic of fractal the Container-Tree has make (3) change into a recurrence expression:

$$k_i = \prod k_{i-1}^{H_{i-1}} \qquad (4)$$

So the self-similarity can be seen in (4)

4. THE COMPONENT REUSING GUIDED BY FRACTAL THEORY

4.1 Assemble Component as the Fractal

In fractal geometry, no matter how complicated the space is, it can be got by a self-similarity stochastic process by using the homologous metric standard.
When we selected some component to construct a system, we can say these components constituted as a self-similarity set. The KrobA method assurance the developing process and the product have the character of strict self-similarity so the whole system can be formalized as a fractal. Combine components as the whole system is a process that taking the components as generators, making use of frame and matching-mapping to mask some characteristic in sub-component that not agree with self-similarity, make use of the iteration function system(ISF) to construct by recurrence way. Then the developing process is product a number of components to overlay the whole problem field with the form of the fractal.

4.2 Component-Dimension

The dimension is an important concept within the fractal theory, it reflect the number of variable that can be used to describe the motion in the space, so the space of n dimensions contain n variables.

At the software engineering, SE realm, we come to modeling to the whole problem field. We take the whole problem space as one component, then overlay whole problem space with a set of component which organized by self-similarity mode. Therefore the parameters that can describe an arbitrary point (a component) in this problem space called Component-Dimension.

The dimension of the component describes the component and the realm space proper to go together with the degree. Taking the whole system as a *Norm-Component*, so the sub-components which spread out by Norm-Component have the same dimension as the Norm–Component. When we select components for software, the components or the component combination must have the same dimension as the realm space.

Then we define the component dimension as follows:
Unit component: The minimum unit of the component can carry on the metric to complications of the component. Then Use the 'L' to represent the complications of the unit component.

Component dimension: Record complications of a component (the Norm- Component) as the 'S',

$$\because K=S/L$$
$$\therefore L^{D} = K \quad (5)$$

D is the Component-Dimension; the dimension of the component not only can be integer, but also can be a fraction too. Logarithm to ① both sides can get the computation formula of the component dimension:

$$D = \text{Log } K / \text{Log } L$$

4.3 The Procedure of Component Reusing
When we want to reusing a component, we must execute a procedure of dimension-turning. Only if we transform a component witch have different dimension form current realm space, this component can be chosen.

Then the procedure of component reusing can be coded as following:

① Input the component;

② Judge the dimension of that component whether have same dimension as the K-Component which it must march. Yes turn to ③, No turn to ④;

③ Though interface-mapping, map the interface-specification of this component to the specification of K-Component.

④ By the construction of several components to implementation the specification of K-Component, then return to ②.

Now we have gotten the strict mathematics definition to judge a component is suitable for reusing or not, then we can decide if it must to develop a new component.

5. CONCLUSIONS

The fractal is a useful mathematics tool that can describe the complicated object. By analyzed the feature of self-similarity in software process and the software products, we can develop a system though component-reusing is the object of component software engineering. In my thesis, KorbA method is the tool that my study to begin with. Though explaining the self-similarity characteristic of component software, elaborate a model for component-reusing. Though inference by strict mathematics to hold the essence of the mechanism of component-reusing.

In the future, we plan to build a perfect mathematics to support large degree reusing. Specific the component software process witch about component-reusing by fractal theory, then create a method for component software evolving.

REFERENCES

[1] Clemens Szyperski, Dominik Gruntz StephanMurer, *Component Software: Beyond Object-Oriented Programming*, Publisher of electronic industries, 2004.

[2] Zhang You Sheng, "The Component Operation and Software Evolves Research," *Computer-Application*, Vol. 24, No. 4.

[3] Ren Hong Min,Qian Le Qiu, "The component constructi-on and its formalizations deduce the research," *Journal of Software*,Vol.14, No.6

[4] She LH, Shen LC, Chang WS, "FBM-Based fractal simulation of terrain," *Journal of Astronautics*, 1999, 20(3):21~25 (in Chinese With English Abstract).

[5] Jiang M, Trajkovic L, "Impact of self2similarity on wireless data network performance," in *Proceedings of ICC2001 Helsinki* , Fin2 land , 2001. 477～481

[6] Atkinson,C, According to the product wireman distance UML method of the component, Machine industry publisher, 2005

Research on Software Architecture and Developing Method Based on Distributed Component *

Juan Li[1], Jiguang Lu[2]
[1]Department of Computer Science and Technology, Northwest Second Nationality Institute
Yinchuan, Ningxia, China
[2]Institute of Computer Science, South-Central University for Nationalities
Wuhan, Hubei, China
Email: [1]lijuannx@sina.com, [2]ljg0101@126.com

ABSTRACT

The idea of component and the architecture of distributed application systems are introduced in this paper. A new B/S architecture based on distributed component, a development framework of application systems, and the process of development are proposed. This can help the programmers to analyze and design distributed software effectively, and then the efficiency of the development can be improved.

Keywords: Distributed Component, Software Architecture, Software Reuse, Distributed Application

1. INTRODUCTION

The experience of software developers and the actual codes are generally provided only for a specific design. Now the complexity of software system becomes more and more high, and the movement of the software personnel becomes more and more frequent. Therefore, how to raise the efficiency and quality of software productions becomes a problem to be solved urgently. At present, the reuse of software based on software component is not only an effective way to support the distributed computation, but also the tendency of the development of the software industry.

2. IDEA OF COMPONENT TECHNOLOGY

2.1 Presentation of Component Technology

For the software development, software reuse includes the reuse of early functions, the reuse of object-oriented language classes, and the reuse of the entire software system components at the Internet Age [1].

The reuse of functions and modules is the idea of developing the structural software. Proper parameters are set for functions to satisfy different requests of the application, while the reuse of modules is implemented by the introduction of the interface specifications. However, structural reuse cannot adapt to the current large scale software development for its bad ability of reuse. The thought of object-oriented software development abstract data and hide information by encapsulation, inheritance and application of classes. Although the inheritance of classes has improved the reuse of codes, it can not escape from the reuse of code level, and the efficiency could not follow the development speed in large scale software developments. Component-oriented technology is carried out through encapsulation on certain functions, and one or more functions of specific services can be completed in this way. Thus software itself can be reused without changing the program. As a result, software can be assembled and ordered as you like as hardware can, which has greatly adapted to the efficiency of software development in nowadays.

2.2 The Basic Concept of Component-based Software Development

Generally speaking, a component is a software unit with integrate semantics, correct grammar and reuse value. It is the system that may be explicitly recognized in the process of software reuse. On the structure, it is a complex of semantic descriptions, communication interfaces and realization codes. Simply speaking, a component is a program body which has special functions, can work independently or cooperatively with other assembled components. The use of components is independent of its development and production. From the view of abstract programming, component reuse has been raised to a higher level than object-oriented technology. A component has encapsulated a group of assembled classes, represents a special task completing one or more functions, and provides multiple interfaces for the user. The entire component hides the concrete realization, and provides the services only through the interfaces.

3. RESEARCH ON SOFTWARE ARCHITECTURE BASED ON DISTRIBUTED APPLICATION

3.1 The Architecture and Component Standard of Distributed Computing Model

In recent years, the component technology has developed rapidly. There formed CORBA of OMG, JAVA platform of SUN, DNA/.NET of Microsoft and Web services of the distributed computing architecture providing software services through standard protocols over Internet.

The foundation of CORBA is object management architecture OMA, in which object request broker ORB is the core of relation model. OMA services are divided into three layers, including CORBA services, CORBA facilities, and Objects of application programs. The architecture of ORB itself is also constituted by three parts: customer interfaces, interfaces of objects implemented, ORB kernel and ORB protocols.

The core components of Windows DNA architecture are a series of system services and application services based on component. These services support open technical standards, which are present as COM form. Microsoft suggests that we should use three layers structure to develop application programs on the architecture and services of Windows DNA. Application is divided into three logical layers: expression, commerce logic and data. After Windows DNA, Microsoft has provided .NET platform. Windows DNA\ .NET is a kind of

∗Supported by the project “A Study on Technologies of Intranet” (MZY00005), Sponsored by the Fund of Natural Science, The State Ethnic Affairs Commission of PR China.
Corresponding Author: Jiguang Lu

architecture which is used to establish tightly coupled distributed application programs.

The main ingredients of J2EE are the following four containers: the application client container, the enterprise JavaBeans container, the Web container, and the applet container. Corresponding to each kind of container, multiple J2EE components (for example, the applet component, the EJB component, the JSP component, the servlet component and application client component) are packed into the module, and handed over in the form of Java Archive (JAR) file.

Web service of the distributed computing system architecture of software service is provided through standard protocols over Internet. Its architecture is a service-oriented architecture that contains three kinds of roles: the service provider, the service requester and the service agent. A component in service-oriented architecture should undertake one or more roles as mentioned above. As the same as object-oriented system, encapsulation, information delivery, dynamic binding, service description and inquiry are the basic concepts of Web service.

3.2 B/S Architecture Based on Distributed Component

The system architecture is the most important factor to make the software system based on component run appropriately and effectively. With the development of network computing technology in distributed environment, three-layer or multi-layer architecture has already been the main pattern of the development of current network application programs, which is of benefit to software reuse. In fact, the B/S architecture is a C/S computation of three-layer architecture, where the original client is replaced by the browser, and the servers are composed of Web server, database server and middleware [2]. Fig. 1 shows B/S architecture based on distributed component.

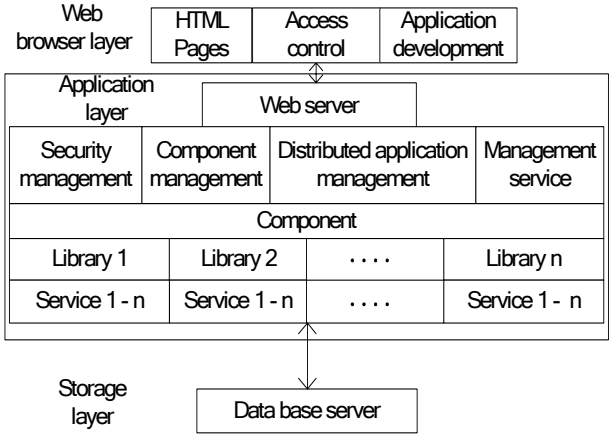


Fig.1. B/S architecture based on distributed component

1) Client/Browser
This layer may respond to the request of a client and visit the special server. It can also get the information about remote objects and hosts, for instance, the name of computers and the name of services etc. Web service of computer server can be invoked by the requesting command with the SOAP protocol format. On the other hand, the data received in the SOAP protocol, format can be interpreted, and the results can be showed to the client in an intuitive way. Additionally, this layer can provide user a tool of building distributed applications, and establishing a multi-project space, so that the user can browse the provided services. Finally, the visual development can be achieved.

2) Application service layer
In this layer, the special functions can be encapsulated according to the way of Web service. When the client invokes a service, the application service will execute corresponding operation right away. The security management module authorizes a client to visit and use a service. According to the mechanism of trust, any client who hasn't been authorized will be refused. There are many component libraries, and each library contains several task services [3]. For example, a mathematics library may contain a lot of mathematical analysis and operation services, and an inquiry library may contain various inquiry services. A library can be distinguished by a name of character string and a unique ID number. Libraries can be added, moved and modified by the distributed system manager in this model. And a lot of information can be stored, such as the load status of the server, the available space of the disk and so on. Every library can be implemented through DLL. A special API is provided for helping developers make their own libraries and services. A developer should declare a name and an ID number, and provide an executive method for every service. The application layer supports the independence of platform well.

3) Storage layer
A lot of data and information can be stored in this layer. So the storage layer can provide good services and necessary data for the component layer upwards.

4. AN OVERALL DEVELOPMENT FRAMEWORK OF APPLICATION SOFTWARE SYSTEM BASED ON DISTRIBUTED COMPONENT

The development of software system based on the distributed component technology mainly lies in carrying out analysis, design, assembly, and combination as well as installation and deployment of components scientifically according to the requirements on the overall software frame foundation. Figure 2 shows the overall development framework.

(1) According to the objective requirements and the architecture of distributed application system, firstly we should decide the style that the development belongs to, such as B/S, C/S, object-oriented style, event-based style or layered system style. Then the function object and its performance can be determined. Therefore, the complexity of system development, management and maintenance can be controlled effectively.

(2) There are four procedures in software development: realization, function testing, reliability testing, and development documentations [4]. We should find the suitable component of architecture before forming component. If there is a component according to the requirements from the available component library, we can acquire directly the reuse component. If the component does not satisfy the requirements, we may correct mistakes on the original component or add new functions, then repackage the component or rewrite an interface to realize the component replacement. The final target of component development is to get the component product, the standard interface and the development documents. The interface must contain attributes of information that records the state of the instance of the

interface, the operations supported by the interface and the invariants of the allowable state restricting the object that supports the interface.

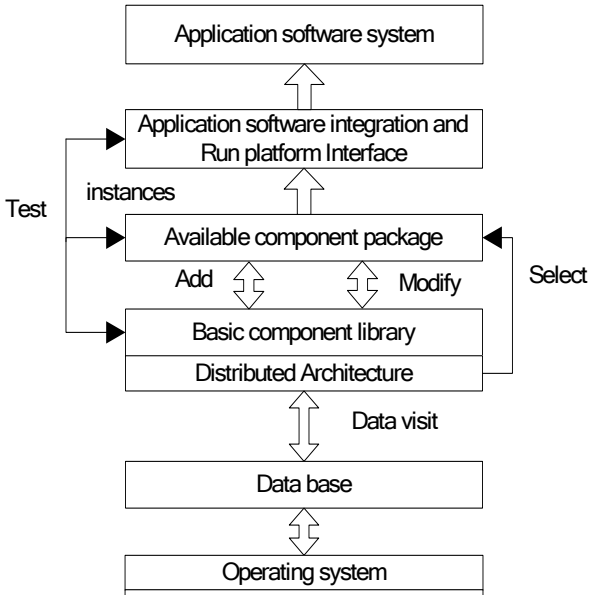


Fig.2. A development framework of application software system based on distributed component

(3) The testing has improved greatly in the procedure of developing application systems. Components need testing in the procedure of building system to handle with problems of potential resource conflicts and incompatibility. System testing includes the function testing and reliability testing. The test should be executed in the target environment or in the simulation environment. Documents should be reserved for integration stage, development stage and maintenance stage of the system.

(4) Under new context, according to architecture of resolving scheme assembling the testing components needs the iteration of integrating, testing, changing components. After that an integrated system is obtained. In Web-based applications the assemble process is to link the application server and the Web server. The component assembly links client's static elements and dynamic elements by generating servlets, active server pages or Java server pages. Choosing method is the detail of Web server. However, for each case, static layout and text information of the Web page should be connected to the content generated dynamically by invoking other components.

(5) At last, an overall system test should be carried out. In this stage, both the function test and reliability test are needed. We should make sure that the system has been satisfied with special requirements. And then defects need adjustment in the actual run until we feel completely satisfied.

5. CONCLUSIONS

The organic combinations in different stages in the software development process have been discussed for the development of application system based on distributed component. The instances will be generated by acquiring the appropriate components, and the system is formed through making use of the state of the art Web-based technology and the development of technologies and applications. This method will be adapted to system evolution in the future. When applications in the same domain are developing, this method will shorten the development time enormously, reduce the administration cost, and lighten maintenance task, which meets the requirements of system development. Nowadays the computer workers have obtained many achievements in this field, but the experiences of effective integration and application are still lacking, which need further studies and discussions.

REFERENCES

[1] Wei Huaying, Zhan Jianfeng, Wang Qin. "Overview of Distributed Component Technologies"[J].*Application Research of Computers*,2004(10),pp. 12~15

[2] Andy S.Y. Lai, A.J.Beaumont, "A Metalevel Component-Based Framework for Distributed Computing Application"[J], *Proceeding of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05)*, OCT,2005,pp.268~293

[3] Dan Grigoras, Stefan Mihaila. "A framework for component-based distributed applications design.The CODE: Component Oriented Distributed Environment"[J].*IEEE Parallel Computing in Electrical Engineering*, 2000.PARELEC 2000. Proceedings. International Conference on, pp.8~12

[4] Xia Cai, Michael R.Lyu, Kam-Fai Wong. "Component-based software engineering: technologies，development frameworks, and quality assurance schemes"[J].*Software Engineering Conference, 2000.APSEC 2000. Proceedings.Seventh Asia-Pacific*, pp.372~379

Juan Li (1975-) is a graduate student of college of computer science, South-Central University for Nationalities. She will graduate in June 2007. She got bachelor's degree in Xi'an University of Science and Technology in 1998. Her research interests are in computer applications and networks.

Jiguang Lu (1943-) is a Full Professor. He graduated from Wuhan University in 1968 as a postgraduate. His research interests are in computer applications, networks, and network security.

Distributed Operating System Techniques

Scheduling Parallel Processes and Load Balancing In Large-scale Computing Systems*

V.P. Kutepov
Applied Mathematics Department, Moscow Power Engineering Institute (Technical University)
ul. Krasnokazarmennaya 14, Moscow, 111250 Russia
Email: KutepovVP@mpei.ru

ABSTRACT

In the paper the problem of the development effective methods and operating tools for management of large-scale computing systems is discussed. In particular scheduling parallel processes and load balancing strategies and algorithms implemented in our projects on software for computing systems are presented.

Keywords: Computing systems, Parallel programming, Scheduling parallel processes, Managing workload

1. INTRODUCTION

The problem of development of strategies and operating tools for effective management of large-scale computing system (CS) is extremely important and very far from satisfactory practical solution [1]. By the existing traditions programmer developing parallel program should take into account the scale of CS (the number of computers or/and processors in it) and adjust granularity of parallelism in a program (or degree of parallelization [1]) and distribute fragments of the program on CS computers in such a way that resources of CS could be used effectively. In essence, nowadays parallel programming process and managing execution of parallel program processes are strongly development on the architecture and scale of CS. Exceptions are probably project of MOSIX [2] and our projects [1, 3, 4] in which the parallel problem of scheduling parallel processes and controlling workload of CS is considered as the central one in providing wide using large-scale CS. At the same time it suggests that architectural solutions in CS organization, in particular in realization of controlling mechanisms, are necessary [1] in order to do much less tedious the work of programmer using large-scale CS.

In the part two of the paper we consider architecture and main components of the management system intended to run effectively parallel programs on CS. The strategies of scheduling parallel processes and controlling workload of CS are discussed in next parts of the paper. The comprehensive version of this paper should be appeared [5].

2. THE ARCHITECTURE AND MAIN FUNCTIONS OF THE CS MANAGMENT

The organization of CS management is a very important aspect in effective realization of scheduling parallel processes and controlling workload of CS. Two boundary strategies of the CS management organization – the centralized and the decentralized have their own merits and shortcomings. The first is more economical from the point of view of the resource maintenance, but becomes a narrow throat at increasing of CS scale [1, 5]. The second lays down the high requirements to the throughput of CS communications and leads to the degradation of the CS operation at increasing data exchanges because of the high time expenses for the realization of the communication functions. The search of the golden mean naturally leads to the hierarchical organization of the large-scale CS management [1].

At the execution of the parallel program on CS the time minimization of its performance is the basic efficiency criterion. However, the same execution time can be reached at the various CS resources, depending on the number of computers (processors) in CS and their average workload. These requirements can be formulated in the following form: $\sum_{i-0}^{N} \frac{1}{T} \int_0^T L_i(t)dt \to \min$, under condition of $T \to \min$. Here $L_i(t)$ - the workload (the fraction of the useful operation) of the i-th computer (processor) of CS at the moment of the time *t*, *T* – the execution time of the parallel program and *N* – the number of CS computers (processors).

The main problem of the workload management usually (and it is not always correct) is formulated as load balancing problem, that is the achievement of the uniform workload of the computing components of CS. We have another point of view at this problem, suggesting that the strategy and algorithms of workload management should minimize negative factors in the CS operation: the idle time of its components, the non-productive delays connected with the swapping in CS computers, the inter-computer exchange and the measurement (see further) of workload parameters and the decision-making about the processes redistribution [1, 4, 5].

Let $L_i(t)$ be the average workload of the i-th computer, which defined as the average workload of its processor by taking into account of its useful operation at some interval $[t-\Delta t, t]$, $L(t) = \frac{1}{N}\sum_{i=1}^{N} L_i(t)$ -the average workload of CS computers CS at this interval. The value $\Delta L_i(t) = L_i(t) - L(t)$ characterizes the relative workload of the i-th computer of CS at the moment t, its negative value suggests that the i-th computer is under-workload at *t*, and the positive value suggests that its workload is upper of the average value. Obviously, the value $\Delta L_i(t)$ divides all *N* computers of CS into two subsets: N_1 – a under-workload subset, and N_2 – the subset of the normally loaded and overloaded computers. $N_1 + N_2 = N$, and the value $\Delta L_i(t)$, $i = 1, 2, \ldots, N$, defines the partial order on these subsets.

Define a set *S(t)* as the union of running $S_1(t)$ and waiting to be run $S_2(t)$ processes in CS at the moment *t*: $S(t)=S_1(t)+S_2(t)$. We call the set $S_2(t)$ the look ahead reserve or supply of ready to run processes. The ability of scheduling processes algorithm to support the number processes in $S_2(t)$ at necessary level is main factor in minimization of standing idle time of CS

* This project is supported by the Russian Foundation for Basic Research (No. 06-01-00817).

computers and as a consequence unproductive use of resources of CS [1, 5]. Two relatively independent subproblems: scheduling parallel processes during parallel program execution on CS and allocation of processes at nodes of CS minimizing the standing idle time are basic in an realization of dynamic management of CS. As it was underlined above the ability of CS management system to support at high level the number of ready to run processes in $S_2(t)$ is important factor in decreasing idle time of the nodes (computers or /and processors).

Consider strategies of the processes reallocation with the purpose to minimize idle time of CS nodes. It is obvious that the situations of low CS workload are the especially actual for the algorithms of CS workload management. Also obviously, that an attempt to redistribute processes in these situations by moving the part of processes of the most loaded computers to the least loaded has not forcible reasons. Firstly, the low workload CS can be caused by the small number processes in $S(t)$, and only the increasing $S(t)$ can change the situation to the best. Secondly, the low workload can be caused by the wrong planning of the processes execution on computers. In particular, a redundancy of processes in the active phase (the execution phase) at computer can lead to the sharp increase of pages exchange with the disk memory (swapping) and to slow down program execution process. It can also be occasioned by the great intensity of the inter-computer exchange, if the processes allocated at computers are needed for very often interaction. Thus, the algorithm of the workload CS management should be so arranged, that at any combination of the specified factors the decision should be directed to increasing number of processes in $S_2(t)$, or to the elimination of other reasons causing the low workload CS, or to that and another simultaneously.

Let's consider the architecture and main functions of the CS management. The general principle of management architecture is a hierarchical decentralized organization when processors of CS are divided into groups (see Fig.1).

In our projects [3, 4] each computer realizes itself the functions of the processes planning. The management of the computers group workload and reallocation of the processes, the reconfiguration of CS, the administration functions and others are performed by the server, obtaining periodically by data about the workload of the computers.

The servers of higher levels perform the similar functions for the subordinated groups of CS. The computer management performs the following functions:

- the control of the processes generation and the processes termination, performance of their interaction with other processes, including being on other computers;
- the planning of processes;
- the parameters measurement of the computer workload, their processing, the forecasting and the transfer to the server;
- the transfer to server the data about its workability;
- the reaction to the server commands.

The group server adjusts the workload of CS computers on the basis of the parameters values of their workload, which is transferred by each computer CS to the server. The same logic of the functions division of the management workloads CS is realized at the following level of the management hierarchy.

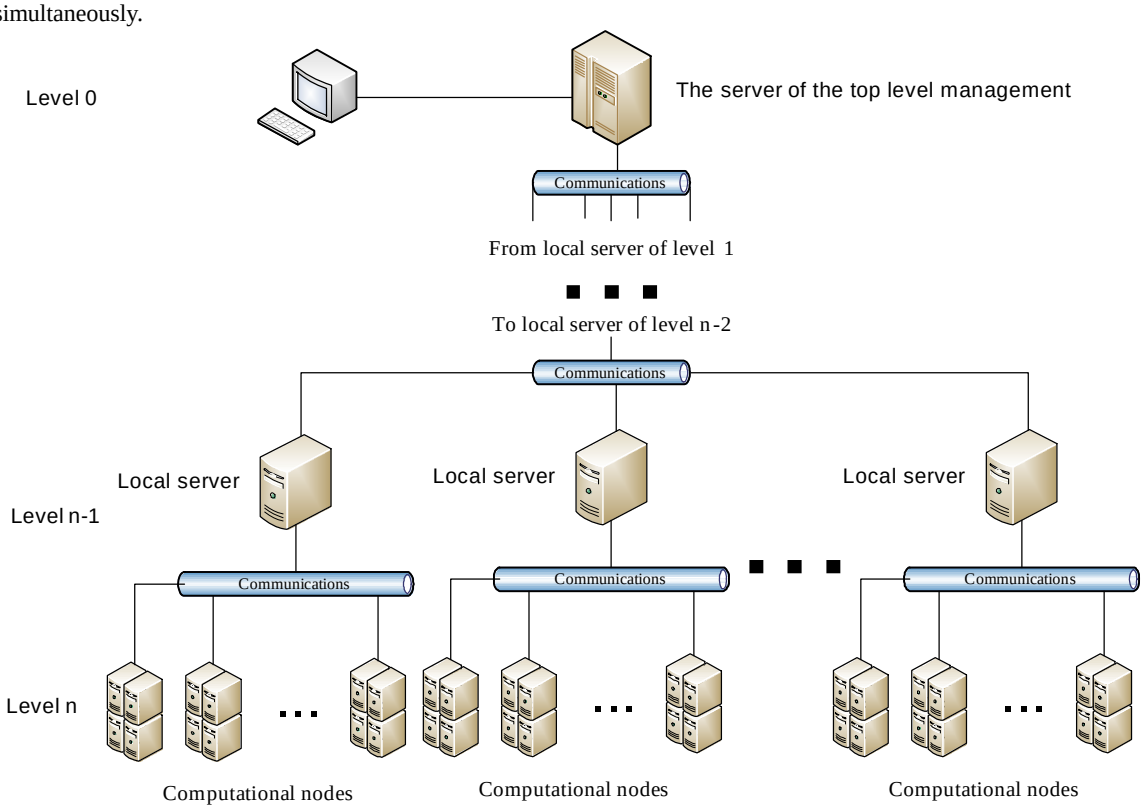


Fig.1. Architecture of CS management

3. SCHEDULING PROCESSES IN COMPUTER OF CS

Let us consider in what way the processes management in working computer or computational nodes of CS should be organized. The contemporary operating systems provide the multi-tasking, using for this purpose the round-robin servicing discipline, which gives the advantage in the execution to short tasks or processes. It is the essential, if the user along with the programs execution carries out the debugging and other procedures and would like to receive the quick reply. This mode of the processes execution is typical for contemporary OS.

In Fig. 2 the scheme of the processes service organization in computers CS is showed, taking in to account imbedded scheduling processes in OS. In the figure 2 the program block of the measurement of the workload parameters (WP), cooperating with the OS, implements the functions of the periodic measurement, the averaging and the forecasting of the computer workload parameters:

- $L_i(t)$ – workload of the i-th computer at the moment t, defined as the workload of its processor (the part time of its useful work);
- $\lambda_i'(t)$ – intensity of the pages exchange with the disk memory;
- $\lambda_i''(t)$ – intensity of inter-computer exchanges;
- $\lambda_i'''(t)$ – intensity of the input-output commands occurrence in the running processes;
- $V_i(t)$ – free memory of the computer;
- $N_{waiting}^{(i)}(t)$ – set of the waiting for the execution processes.

An interpreter (IN) of the parallel programs places the processes induced during execution of a program on processor (PR) in the queue $N_{waiting}$. A scheduler (SH) removes a part of these processes to the queue N_1 from which PR takes processes for execution in the round-robin order. The processes in the queues N_3, N_4, N_5 are waiting for execution of the exchange of pagers with disk memory (D), the inter-computer data exchange (IE) and input/output (I/O) respectively. The SH can delay a part of being executed processes and place them in the queue N_2 in a case if a number of active processes $N_{active}=N_1+N_2+N_3+N_4+N_5$ is redundant and high swapping (great value of λ_i') is provoked.

The developed algorithm of scheduling processes in a computer of CS is given at Fig. 3. At this figure $\alpha_i = \lambda_i'/\mu_i$ - loading factor of the paging system (μ_i – paging system capacity). A – some experimentally derived threshold constant, by which the level of the computer workload is regulated.

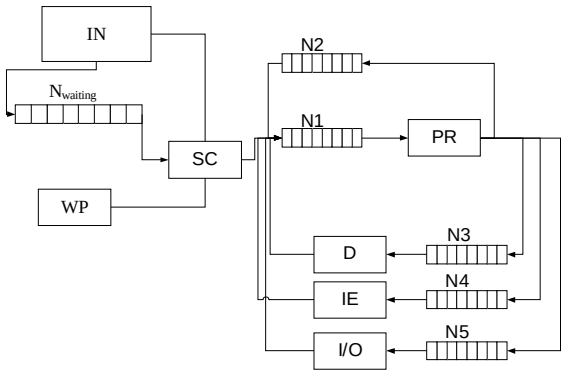


Fig.2. The organization of the processes execution in the computer

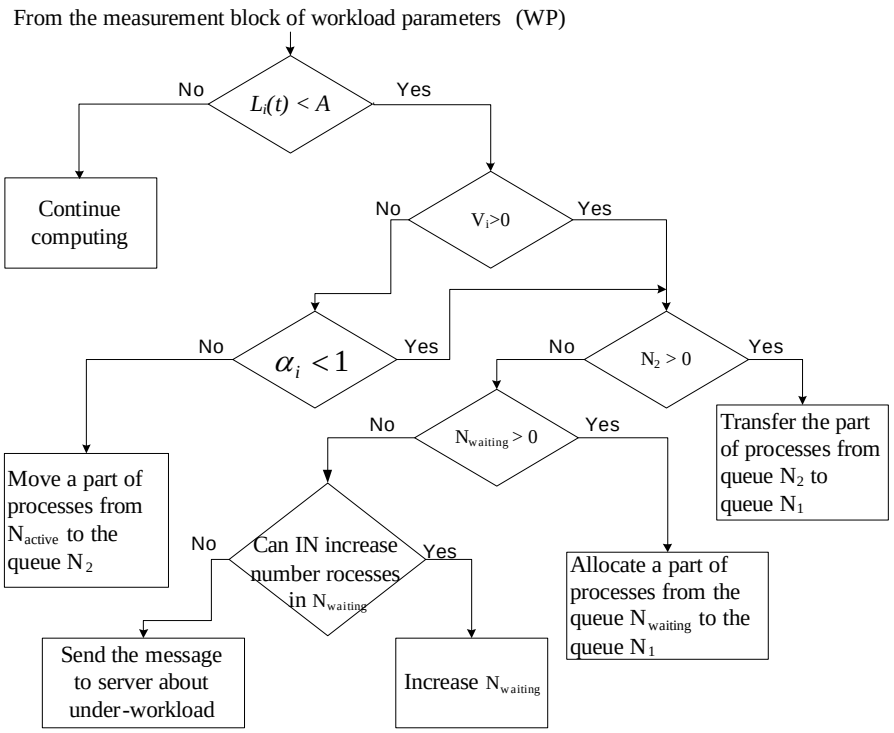


Fig.3. Scheduling processes in the computer

4. SERVER FUNCTIONS IN MANAGING CS WORKLOAD

The server is intended for the regulation of the CS computers workload, aiming to minimize the idle time of the processors due to the dynamic redistribution of the processes and the increasing the number of ready for execution on processes. The server periodically obtains the data about the workload of its subordinated computers and forecasts its change [6]. The scheme and the logic of the server interaction with the group computers are shown in the Fig. 4.

In the figure 4 the designations A and B on the arrows show the possible alternatives of the corresponding decisions about the redistribution of processes between computers during their dialogue with the server. In fig. 4 all parameters of the workload represent the averaged values on some interval and the forecast is the predicted values change of the same parameters.

The problem of the accurate measurement of the workload parameters is very important factor in scheduling processes and managing workload in CS [6, 7].

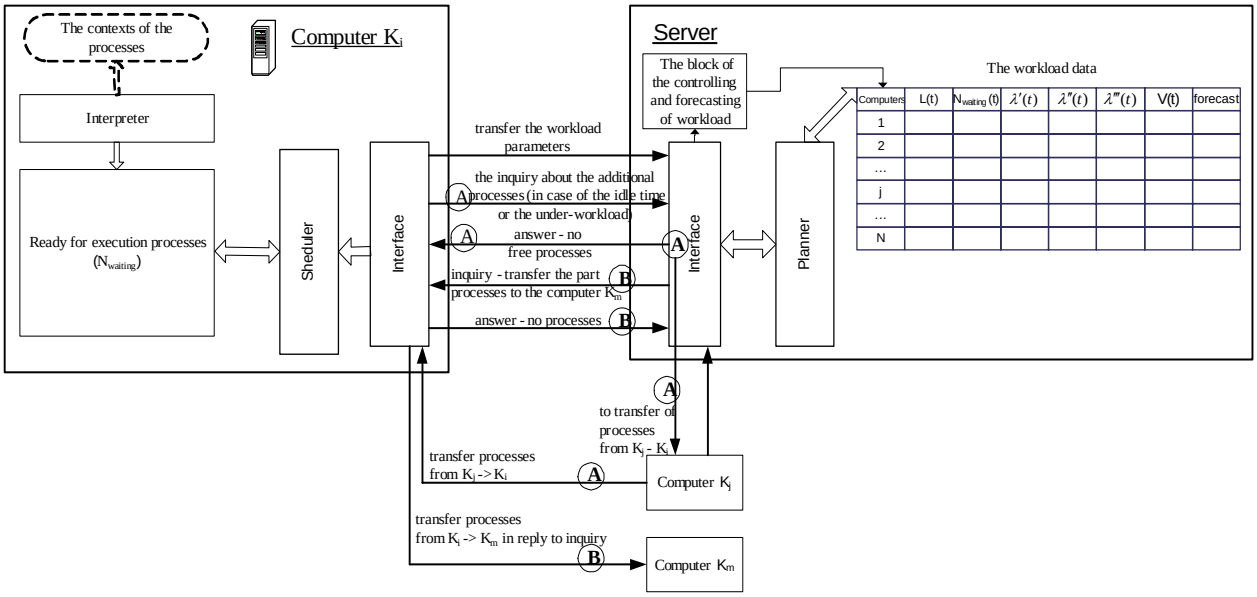


Fig.4. The interaction scheme of the server with computers

We performed wide the experimental investigation in order to better understand stochastic nature and the most significant parameters which characterize a behavior of the processes in CS [5, 6]. As the result we developed the simple measurement and prediction workload parameters algorithms with small time consuming for their operation.

5. CONCLUSIONS

On the basic of the developed algorithms preliminary experimental work on cluster of 64 processors was done. The results show that it is possible to decrease up to 50% the execution time of complicated parallel programs using proposed algorithms. The algorithms were implemented in our flowgraph stream and functional parallel programming systems [3, 4].
The problem of static planning parallel execution of flowgraph programs is considered in paper [8].

REFERENCES

[1] Kutepov V P, On Intelligent Computers and Large New-Generation Computer Systems. Journal of Computer and Systems Sciences International, Vol. 35, No. 5. 1996。

[2] Barak A, Laadan O, *The MOSIX multicomputer operating system for high performance cluster computing*. http://www.cs.huji.ac.il/mosix

[3] Kotlyarov D V, Kutepov V P, Osipov M A, “Flowgraph Stream Parallel Programming and Its Implementation on Cluster Systems”, *Journal of Computer and Systems Sciences International*, 2005, Vol. 44, No. 1, pp. 70-89.

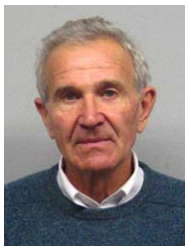
[4] Bazhanov S E, Vorontsov M M, Kutepov V P and Shestakov D A, “Structural analysis and planning of processes of parallel execution of functional programs”. *Journal of Computer and Systems Sciences International*, 2006, Vol. 44, No. 6, pp. 947-957.

[5] Kutepov V P, “Intelligent scheduling processes and controlling workload in the large computing systems”. (to appear in *Journal of Computer and Systems Sciences International*, 2007, No. 5).

[6] Kutepov V P, Kotlyarov D V, The workload management of the cluster systems (in Russian). *Proceeding of the Fourth International Scientifically-practical Seminar and the All-Russia Youth School*. The Samara Center of Science of the Russian Academy Sciences, 2004.

[7] Dr. Neil Gunther Load, Average Part I: How It Works. TeamQuest Corporation, 2005.

[8] Kutepov V P, Makarievskiy S N, Parallel Processes Execution Planning in Computing Systems and GRID Computing on the Base of Flowgraph Stream Parallel Programming, *2007 International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, August 14-17, 2007, YiChang, HuBei, China.



Vitaliy Pavlovich Kutepov is a Doctor of Technical Science and an Honored Professor, the Vice-Chair of the Applied Mathematics Department at Moscow Power Engineering Institute (Technical University) (MPEI) He graduated from MPEI in 1961 with the specialty “Computer Science”. In 1968 he obtained the Ph.D. on the theme “Research of Some Formal Methods of the Description and the Optimization of Computing Processes”. In 1982 he won the Doctor's Degree on the theme “Functional Systems and Parallel Computing”. From 1987 to 2003 he was the Head of the Applied Mathematics Department in MPEI. He was visitor of Mathematical and Computing Center of Amsterdam (1972), Department of Computer Science at Ediburgh University (1986), Department of Computer Science at Manchester University (1992). He is one of the founders of network MPEI, and the head of “the Center of Supercomputer Technology”. He has published over 100 scientific journal papers and books, and trained 22 doctors of technical science. His research interests are in the theory of parallel programming, the management of parallel processes in large computer systems, the logical models and languages, the theory of the directed relation, the functional models and languages of parallel programming and the architecture of computer systems.

Towards Dynamic Integration and Scheduling of Scientific Applications

Lei Yu, Frédéric Magoulès
Applied Mathematics and Systems Laboratory, Ecole Centrale Paris
Grande Voie des Vignes, 92295 Châtenay-Malabry Cedex, France
E-mail: lei.yu@ecp.fr, frederic.magoules@hotmail.com

ABSTRACT

One of the challenges of Grid computing is the integration of legacy scientific applications. There is no standard way of registering these applications, describing their input parameters and output results and monitoring their progress in the Grid environment. The Web Services Architecture (WSA) is an ideal technology to integrate legacy applications into the Grid. Adopting this service-oriented model, a framework is here presented and implemented to achieve the dynamic deployment and scheduling of scientific applications. The framework treats all components (Computing Resource and Mate-Scheduler) as WSRF-compliant services which support the applications integration with underlying native platform facilities and facilitate the construction of the hierarchical scheduling system.

Keywords: Web services, WSRF, Dynamic Deployment, Application Integration, Meta-Scheduler

1. INTRODUCTION

Computational Grids have become an important asset in large-scale scientific and engineering research. Many scientific communities are feeling a growing need to integrate their legacy applications into grid environment. Unfortunately, there is no standard way of integrating these applications into a Grid so that they can be discovered by interested clients and end-users [1]. By wrapping command-line applications into Grid services and scheduling these Grid services for end-users, a framework is here presented and implemented to enable the dynamic deployment, the discovering and the submission of scientific applications in a Grid environment.

A Grid service is a Web service that provides a set of well-defined interfaces and that follows specific conventions. The interfaces address discovery, dynamic service creation, lifetime management, notification, and manageability; the conventions address naming and upgradeability [11]. In our framework, the scientific applications are described as job description files in XML format [2]. The WSRF resource [3] is used to contact a local job manager through Globus [4] to submit the legacy application. The framework has three primary components:

- The *Resource Service* is deployed in each computing resource. It manages all the application descriptions and has a mechanism to monitor the creation, deletion, and modification of the application description. A uniform interface is provided for the client to invoke the applications in the computing resource and to monitor the status of application executions.
- The *Meta-Scheduler* is deployed as a Grid services scheduler in our framework. The *Meta-Scheduler* manages and monitors all available computing resources in a VO [5]. Via the uniform interface of *Resource Service*, the *Meta-Scheduler* collects the dynamic and static information of computing resources to make scheduling decisions, creates WSRF resources for users, submits applications and monitors the execution status.
- The *AdminTool* can interact with *Resource Service* in a secure way. The *AdminTool* has a graphic interface and can be used to add, delete and modify the application descriptions by the local administrator.

In this paper, our primary focus is the architecture and the implementation of the framework. The plan of the paper is as follows. In Section 2 the model architecture is described. The implementation aspects are presented in Section 3. In Section 4 two experimentations are presented to evaluate the performance of the framework. Finally we conclude with a brief discussion of the future research.

2. MODEL ARCHITECTURE

The Web Services Architecture (WSA) adopts a common representation for computational and storage resources, networks, programs, and databases. All are treated as services–network-enabled entities that provide some capability through the exchange of messages. Adopting this uniform service-oriented model makes all components of the environment virtual through encapsulation of diverse implementations behind a common interface [12]. Our framework adopts this service-oriented model and wraps scientific applications in WSRF-compliant services.

Fig. 1 illustrates the architecture of the model. The *Resource Service* is deployed in each Computing Resource and makes the Computing Resource virtual through encapsulation of scientific applications behind a common interface (Applications Interface). *User Applications* interact with the *Meta-Scheduler*, via a uniform *User Interface*, to discover applications, to submit applications and to monitor execution status. The architecture treats all components (Computing Resource and Mate-Scheduler) as WSRF-compliant services which support applications integration with underlying native platform facilities and facilitate the construction of hierarchical scheduling system.

2.1 Applications Management

The ability to dynamically deploy and to discover the wrapped applications must be achieved by the framework. In the *Resource Service*, the scientific applications are described in the Job Description Schema [6]. An *Applications Manager* takes the responsibility to add, delete and modify application descriptions in a *Storehouse*. An *AdminTool* can be used by the local administrator to interact with the *Applications Manager*.

When the local administrator uses the *AdminTool* to add, delete and modify the application descriptions, the *Applications Manager* updates the application list and modifies the job description files in the application storehouse. It sets also a signal to notify the *Meta-Scheduler* the modification of the application list. The *Mate-Scheduler* monitors the signal status. When it detects the change of signal status, it updates its application lists within a reasonable delay.

According to the request of user applications, the *Meta-Scheduler* queries the applications lists which are copied from each *Resource Service*. If there is more than one *Resource Service* which deploys the wanted application, a scheduling decision is made by the *Meta-Scheduler*.

2.2 MDS and Scheduling

MDS can be configured in a hierarchical fashion with upper levels of the hierarchy aggregating information from the lower-level MDS (Index Services) [7]. Thus from each Computing Resource, the *Meta-Scheduler* can gather the dynamic and static information for the scheduling decision.

A simple scheduling algorithm is implemented in the *Meta-Scheduler*. When the *Meta-Scheduler* finds that there is more than one available *Resource Service* which conforms to the user requirement, it compares the number of available CPUs of each *Computing Resource*. The *Meta-Scheduler* selects the resource which has the most available CPUs. If the number of

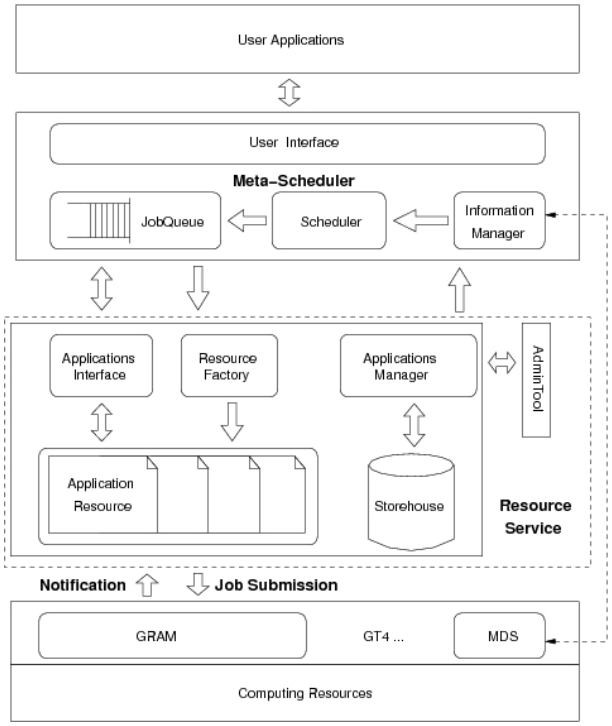


Fig.1. The Architecture of the Proposed Model.

available CPUs is similar, the *Meta-Scheduler* calculates the value of **WaitingJobs / TotalCPUs** for each *Computing Resource*. **WaitingJobs** is the number of jobs waiting in the local job queue, and **TotalCPUs** is the number of CPUs on each *Computing Resource*. The resource which has the smallest value is selected. A scheduling algorithm which is more complex will be considered in the future.

2.3 Standard Interface for Application Arguments

In the Job Description Scheme, there are three elements: *Argument*, FileStageIn and *FileStageOut* [6]. After a *Resource Service* and a application description have been selected by the *Meta-Scheduler*, the user specifies all the input parameter values (include *Argument*, *FileStageIn* and *FileStageOut*) and sends a submission request to the *Meta-Scheduler* via *User Interface* of the *Meta-Scheduler*. Then the *Meta-Scheduler* creates a replica of selected application description, sets these elements in this Job Description replica and inserts this replica in a *JobQueue*. In the *JobQueue*, a scheduling strategy of FCFS (First Come First Serve) is adopted to really submit this Job Description to the GRAM service of the *Computing Resource*.

3. SERVICES IMPLEMENTATION

The *Mate-Scheduler* and *Resource Service* are implemented in the base of GT4 and WSRF. The PortType [13] of each Service is illustrated in Table [1,2].

Table 1. the PortType of Meta-Scheduler.

	PortType	Description
1	openSession	Open a session for a user. It returns a client number to the user, and the user uses this number to query the job status.
2	closeSession	Close the user session. If the job is finished, the user uses this PortType to close his account.
3	findApplication	The operation is used by user applications to search the needed application in each Resource Service. If there are more than one Resource Service which has the needed application, the Meta-Scheduler uses MDS information to select the best resource for user.
4	Scheduler	Submit the selected Job Description to a Resource Service.
5	getJobStatus	Get the job execution status.

3.1 Job Submission Sequence

The *Mate-Scheduler* and *Resource Service* are implemented on the basis of GT4 and WSRF. Fig. 2 illustrates the sequence of a user job submission.

- The user invokes the *openSession* operation of the *Meta-Scheduler* to get a client number.
- The user invokes the *findApplication* operation with client number and the requested application as parameters.
- The *Meta-Scheduler* searches in all the application lists. If it finds the requested application, a Boolean "true" is returned to the user.
- The user gets "`true", so it can invoke the *scheduler* operation in order to submit the application.
- The *Meta-Scheduler* invokes *createResource* of the *Factory Service* to create a resource for the user.
- After having created the resource, the *Meta-Scheduler* submits the job to *Resource Service*
- The user uses *getJobStatus* to query the job status.
- If the execution of application is finished, the user invokes *closeSession* to destroy the session.

Table 2. The PortType of Resource Service

Component		PortType	Description
Resource Factory	**1**	getApplicationList	It is used by the Meta-Scheduler to get the application list from each Resource Service.
	2	createResource	According the user's request, it creates a application resource Application Interface
Applications Interface	**3**	submit	It is used to submit the Job Description to the GRAM service.
	4	4 getJobStatus	Get the job execution status
Applications Manager	**5**	addApplication	Add Job Description (used by dminTool)
	6	modifyApplication	Modify Job Description (used by AdminTool)
	7	deleteApplication	Delete Job description (used by dminTool)
	8	isApplicationChanged	Detect the change of application list

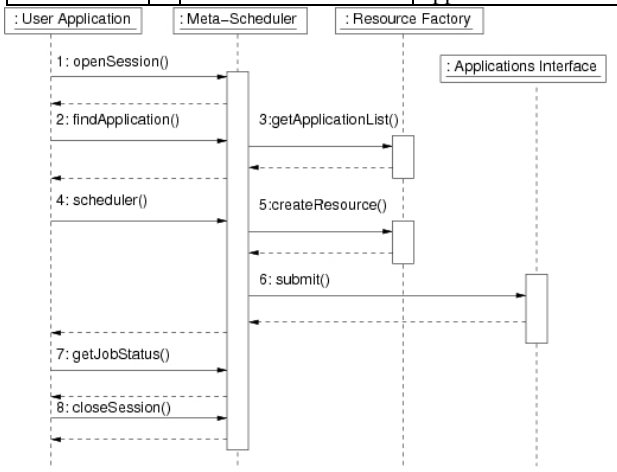


Fig 2. the Sequence Diagram for a User Job Submission.

3.2 Security

The framework deals with the two basic concepts of security: authentication (verifying that users are who they say they are) and authorization (assigning privileges to users once their identity has been firmly established). To enforce security on the client-side, applications which interact with *Meta-Scheduler* and *Resource Service* must be configured to use host authorization and to enforce both privacy and integrity authentication. On the server-side, authentication and authorization are specified by creating a security descriptor file before services (*Meta-Scheduler* and *Resource Service*) are compiled into GAR files [8]. The Gridmap authorization is adopted instead of host authorization on the server-side.

4. EVALUATION

In the proposed framework, the capacity of dynamic deployment and the performance of the uniform interface must be evaluated. The most important aspect for the job submission is the turn-around time. Turn-around time is the time from a job being accepted by the Meta-Scheduler till the completion (i.e. the job has reached the done state). The turn-around time is measured in 2 cases:

• An application is added dynamically in a *Resource Service*.
• Our framework and **globusrun-ws** [9] are used to submit jobs to a same Computing Resource. A comparison is made to evaluate the different performance between our framework and **globusrun-ws**.

4.1 Dynamic Deployment Experiments

The *AdminTool* is used to add dynamically an application in the system. The experimental setup is as follows. The *Resource Service* is deployed and tested at two Condor clusters: a cluster named C1 with three servers, another cluster named C2 with two servers. Each server has 2 Pentium 4 3.20GHz with 1 GB RAM. The *Meta-Scheduler* is installed in a PC powered by Pentium 4 3.00GHz with 512 MB RAM. All the machines are connected by 100 Mb Ethernet. GT 4 is installed in the central manager of Condor pool, and Scheduler Adapters are configured to support the job submission into the Condor pool. From a laptop, the user application submits 30 jobs to the *Meta-Scheduler* and the interval of submission is 30 seconds. The application is a simple C program. It waits 5 minutes and then returns. In order to execute the application in the standard universe, condor compiler must be used to re-link the application with the Condor libraries [10]. After the user has submitted 8 jobs, the local administrator of C2 runs *AdminTool* to add the application in C2. For comparisons, the user application submits 30 jobs once again. The difference with the first time is there is not a dynamic deployment, thus only C1 is used to submit jobs.

Fig. 3 shows that the turn-around time of followed jobs dropped down when the application is added in C2 (after eighth job). Because the *Meta-Scheduler* detects the modification of applications list in C2 and it can submit the user job to C2. Thus the ninth job does not wait to be submitted to C1; instead it is submitted to C2 and is executed immediately. Since the system MDS takes time to gather

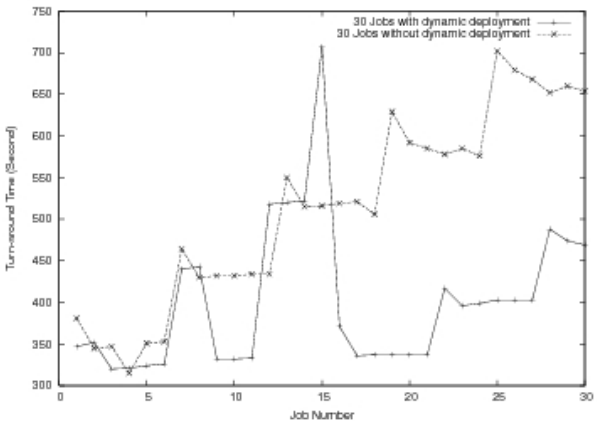


Fig.3. The Performance of Dynamic Deployment of Application.

resource information, the *Meta-Scheduler* uses the information a little delayed to schedule the jobs. When the fifteenth job is

submitted, the *Meta-Scheduler* submits continually the job to C2, because the *Meta-Scheduler* thinks that there are still some free CPUs in C2. This is the reason why the turn-around time of the fifteenth job is a little longer. After the submission of the fifteenth job, the turn-around time of followed jobs in the case of dynamic deployment is much more dropped than in the case of the absence of dynamic deployment because of the distribution of job on two clusters.

4.2 Comparison between the Framework and Globusrun-Ws

In order to evaluate the performance of the framework, a comparison is made by submitting jobs to the Computing Resource, C1, via different interface (our *Resource Service* and **globusrun-ws** [9]). A user program is applied to submit jobs via the *Resource Service* and the interval of submission is 30 seconds. The application which the user needs is only deployed on C1. Thus the user jobs can solely be executed on C1. When **globusrun-ws** is used to submit a job, it returns till the completion of this job. Therefore in the program which uses **globusrun-ws** to submit jobs every 30 seconds, each execution of **globusrun-ws** is started in a thread. The program monitors the status of threads and when a thread is no longer alive, this meant the job execution is finished. Then the program calculates the turn-around time for each completed job.

Fig. 4 shows the result. It is shown that the turn-around time in the case of *Resource Service* is a little shorter than the time in the case of **globusrun-ws**. But the performances of the two infrastructures are very close.

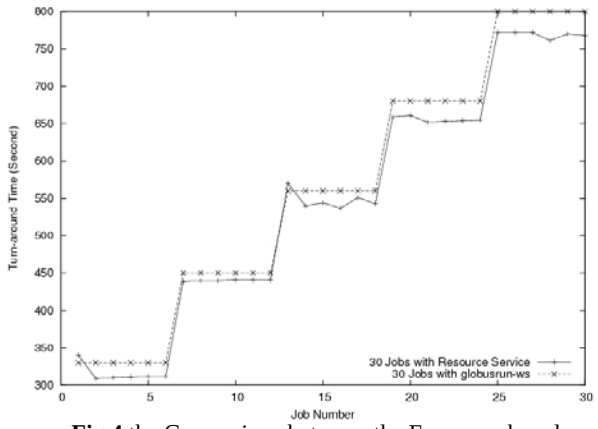


Fig.4.the Comparison between the Framework and Globusrun-Ws.

5. RELATED WORK

In the context of Computational Grids, we can mention the following meta-scheduling projects : Condor/G [14], which provides user tools with fault tolerance capabilities to submit jobs to a Globus based Grid; Nimrod/G [15], designed specifically for Parameter Sweep Application (PSA) optimizing user-supplied parameters like deadline or budget; GridLab Resource Management System (GRMS) [16], which is a meta-scheduler component to deploy resource management systems for large scale infrastructures; and the Community Scheduler Framework (CSF) [17], an implementation of an OGSA-based meta-scheduler; and the Enabling Grids for E-sciencE (EGEE) Resource Broker [18], that handles job submission and accounting. Finally, GridWay gives end users, application developers and managers of Globus infrastructures a scheduling functionality similar to that found on local DRM systems, including the support for DRMAA GGF standard [19].

There are several research efforts aiming at automating the transformation of legacy code into a Grid service. Most of these solutions are based on the general framework to transform legacy applications into Web services outlined in [20], and use Java wrapping in order to generate stubs automatically. One example could be found in [21], where the authors describe a semi-automatic conversion of legacy C code into Java using JNI (Java Native Interface).

Compared to Java wrapping, some solutions [1], [22], [23] are based on a different principle. They offer a front-end Grid service layer that communicates with the client in order to pass input and output parameters, and contacts a local job manager to submit the legacy computational job. The Grid service is defined by OGSA [24] which supports, via standard interfaces and conventions, the creation, termination, management, and invocation of state-full and transient services as named and managed entities with dynamic and managed lifetime. To deploy a legacy application as a Grid service there is no need for the source code. The user only has to describe the legacy parameters in a pre-defined file (description) and to transfer that file to a Factory service. But, the interface by which we can interact with the deployed applications is not uniform, because the Factory needs a description of the service to create an instance of application. The different description providers could define various service port-types in the descriptions. Therefore the interface of application instance varies according to different service port-types. The other problem is the quantity of service instances. The application is created and deployed as service instance. In this case, if we deploy a large quantity of needed applications in a computing resource, there will be too many service instances to be created. The management of these instances is truly a delicate job.

The paper [25] presents a lightweight Grid solution for the deployment of multi-parameters applications on a set of clusters protected by firewalls. The system uses a hierarchical design based on Condor for managing each cluster locally and XtremWeb for enabling resource sharing among the clusters. This approach fulfills the requirements of Grid deployments ensuring strong security and fault tolerance using resilient components which fetch their context before restarting.

6. CONCLUSIONS

The framework for dynamic deployment of scientific applications into grid environment has been described. The framework addresses dynamic applications deployment. The local administrator can dynamically put some applications available or unavailable on the *Grid Resource* without stopping the execution of the Globus Toolkit Java Web Services container. A *Grid Scheduler* has been integrated in the framework, which can realize simple job scheduling, select the best *Grid Resource* to submit jobs for the users. The performance of the framework has been evaluated by some experiments. All the components in the framework are realized in the standard of Web Service, so the other meta-schedulers or clients can interact with the components in a standard way.

We plan to complete the Grid Scheduler to realize more complex scheduling algorithm and to integrate the workflow.

The Grid Scheduler is a Web Service. The interaction between the Grid Scheduler or between a Grid Scheduler and the other meta-scheduler can be realized in the standard of Web service. So we would like to create a hierarchy of meta-Scheduler to realize a distributed scheduling.

REFERENCES

[1] Gopi Kandaswamy, Liang Fang, Yi Huang, Satoshi Shirasuna, and Dennis Gannon. A generic framework for building services and scientific workflows for the grid. In The 2005 *ACM/IEEE Conference on SuperComputing*, 2005.

[2] Vladimir Silva. Quick start to a GT4 remote execution client, 2006. Available online at: http://www-128.ibm.com/developerworks/grid/library/gr-wsgram/ (accessed 27 May 2007).

[3] Borja Sotomayor. The Globus toolkit 4 programmer's tutorial.

[4] Globus Team. Globus toolkit. http://www.globus.org.

[5] Ian Foster, Carl Kesselman, and Steven Tuecke. The anatomy of the grid: Enabling scalable virtual organizations. International *Journal of High Performance Computing Applications*, 15(3):200–222, 2001.

[6] Globus Team. Gt 4.0 ws gram: Job description schema doc, Available online at: http://www.globus.org/toolkit/docs/4.0/execution/wsgram/schemas/gram_job_description.html (accessed 27 May 2007).

[7] Jeff Mausolf. Grid in action: Monitor and discover grid services in an soa/web services environment, 2005. Available online at: http://www-128.ibm.com/developerworks/grid/library/gr-gt4mds/index.html (accessed 27 May 2007).

[8] Babu Sundaram. Introducing gt4 security, 2005. Available online at: http://www.128.ibm.com/developerworks/grid/library/gr-gsi4intro/ (accessed 27 May 2007).

[9] Globus Team. globusrun-ws - Official job submission client for WS GRAM. Available online at: http://www.globus.org/toolkit/docs/4.0/execution/wsgram/rn01re01.html (accessed 27 May 2007).

[10] Condor Team. Condor user's manual. Available online at: http://www.cs.wisc.edu/condor/manual/v6.8/2_4Road_map_Running.html (accessed 27 May 2007).

[11] Foster, I., Kesselman, C., Nick, J., Tuecke, S.: Grid services for distributed system integration. *IEEE Computer* 35:37–46, 2002.

[12] Foster, I., Kesselman, C., Nick, J.M., Tuecke, S.: Grid services for distributed system integration. *Computer* 35(6):37–46, 2002.

[13] W3C: Web services description language (wsdl) 1.1, Available online at: http://www.w3.org/TR/wsdl.

[14] Frey, J., Tannenbaum, T., Livny, M., Foster, I., Tuecke, S.: Condor-G: A computation management agent for multi-institutional Grids. *Cluster Computing*, 5(3): 237–246, 2002.

[15] Buyya, R., Abramson, D., Giddy, J.: A computational economy for Grid computing and its implementation in the Nimrod-G Resource broker. *Future Generation Computer Systems*, 18:1061–1074, 2002.

[16] Seidel, E., Allen, G., Merzky, A., Nabrzyski, J.: GridLab–A Grid application toolkit and testbed. *Future Generation Computer Systems*, 18(8):1143–1153, 2002.

[17] Platform Computing team: Open source metascheduling for virtual organizations with the community scheduler framework (CSF). *Technical report*, Platform Computing, 2003.

[18] EGEE Team: EGEE middleware architecture and planning (Release 2). *Technical report*, DJRA1.4, EGEE, 2005.

[19] Huedo, E., Montero, R.S., Llorente, I.M.: A modular meta-scheduling architecture for interfacing with pre-WS and WS Grid resource management services. *Future Generation Computer Systems*, 23, 252–261, 2007.

[20] Kuebler, D., Eibach, W.: Adapting legacy applications as web services. IBM DeveloperWorks, 2002. Available online at: http://www-128.ibm.com/developerworks/library/ws-legacy/.

[21] Huang, Y., Taylor, I., Walker, D., Davies, R.: Wrapping legacy codes for grid-based applications. In: *Parallel and Distributed Processing Symposium*, 2003. Proceedings. International. (22-26 April)

[22] Kacsuk, P., Goyeneche, A., Delaitre, T., Kiss, T., Farkas, Z., Boczko, T.: High-level grid application environment to use legacy codes as ogsa grid services. In: Grid Computing Proceedings. *Fifth IEEE/ACM International Workshop*, 428–435, 2004.

[23] Gannon, D., Ananthakrishnan, R., Krishnan, S., Govindaraju, M., Ramakrishnan, L., Slominski, A.: Grid web services and application factories. Computing: Making the Global Infrastructure a Reality. Fox, Berman and Hey, eds.*Wiley*, 2003.

[24] Foster, I., Kesselman, C., Nick, J., Tuecke, S.: The physiology of the grid: An open grid services architecture for distributed systems integration, 2002.

[25] Lodygensky, O., Fedak, G., Cappello, F., Neri, V., Livny, M., Thain, D.: Xtremweb & condor : sharing resources between internet connected condor pool. In: Cluster Computing and the Grid. Proceedings. CCGrid 2003. *3rd IEEE/ACM International Symposium*. (12-15 May 2003) 382–389, 2003.

Task Scheduling by Limited Duplication on a Bounded Set of Heterogeneous Processors*

Fei Yin, Xiaoli Du, Changjun Jiang, Rong Deng
Department of Computer Science and Technology, Tongji University
the Key Laboratory of "Embedded System and Service Computing", Ministry of Education
Shanghai, 201804, China
Email:yinfei-mailbox@163.com, hhaafy@hotmail.com, du_xiaoli121@hotmail.com,cczyl@mail.tongji.edu.cn

ABSTRACT

This paper addresses the static scheduling of a directed acyclic task graph (DAG) on a heterogeneous, bounded set of distributed processors to minimize the makespan. By analyzing the task scheduling model, we present a new heuristic, known as Dynamic Critical Path Duplication (DCPD), for scheduling DAG on a set of heterogeneous processors. DCPD assigns the tasks on the dynamic critical path to the suitable processor which minimizes the earliest finish time for them, combining insertion-based scheduling and task duplication techniques. The comparison study by simulation on Simgrid, based on randomly generated DAG, shows that DCPD surpasses previous approaches in terms of both quality and cost of schedules, which are mainly presented with schedule length, frequency of best result, and scheduling time metrics.

Keywords: Parallel Computing, Task Scheduling, DAG, Cluster Based Scheduling, Duplication Based Scheduling, Simgrid

1. INTRODUCTION

A parallel computing system is characterized by multiprocessor executing parallel jobs. Heterogeneity in a multiprocessor system is introduced due to the presence of processors that have different characteristics, including speed, memory space, special processing functionalities, etc. In the parallel system, an efficient task partitioning and scheduling strategy has been regarded as one of the important issues. The task partitioning strategy divides an application into tasks of appropriate grain size and an abstract model of such a partitioned application can be represented by a directed acyclic graph (DAG).

The general task scheduling problem includes the problem of assigning the tasks of an application to the suitable processors and the problem of ordering task executions on each resource. When the structure of the parallel program in terms of its task execution time, task dependencies, task communication and synchronization, is known a prior, scheduling can be accomplished statically at compile time. The objective of scheduling is to minimize the completion time of a parallel application by properly allocating the tasks to the processors.

The problem of optimal scheduling of tasks with required precedence relationship, in the most general case, has been proven to be NP-complete and optimal solutions can be found only after an exhaustive search. Such optimality can be achieved if adequate time is available, i.e., the problems are non-real-time type. Hence, many heuristics that could give an optimal solution in polynomial time have been proposed, for some very restricted cases. But, approximate optimizations are sometimes said to be an acceptable approach that can be put forth for the scheduling problem. Because of its key importance on performance, the task scheduling problem in general has been extensively studied and various heuristics are proposed in the literature. These heuristics are classified into a variety of categories, such as list scheduling algorithms [5], clustering algorithm [3], duplication based algorithm [4], and guided random search methods [6].

In this paper we propose a compile-time task scheduling algorithm based on cluster scheduling and duplication algorithm. The algorithm works under the environment of a bounded number of fully connected heterogeneous processors. The remainder of the paper is organized as follows: Section 2 introduces the model of the task scheduling for heterogeneous computing; Section 3 presents the DCPD algorithm. Section 4 briefly reviews some other scheduling algorithms that we apply for performance comparison and the simulation results on Simgrid are also presented. Section 5 concludes the whole paper.

2. TASK SCHEDULING MODEL

The complete task scheduling model for heterogeneous computing consists of the processor model and the task model.

2.1 The processor model

The processor model $PE = (P, S, Lm, B)$ is a network of heterogeneous processors connected in a fully connected topology in which all inter-processor communications are assumed to perform without contention. In our model, it is also assumed that computation can be overlapped with communication.

$P = \{p_i; i \in [1, M]\}$ is the set of processor.

$S = \{s_i; i \in [1, M]\}$ denotes the computing speed of p_i.

$Lm = \{a_i; i \in [1, M]\}$ denotes the I/O setup overhead for p_i.

$B = \{b_{i,j}; i, j \in [1, M]\}$ denotes the bandwidth between p_i and p_j.

2.2 The Task Model

In the general form, the application for scheduling can be expressed as a directed acyclic graph (DAG). A node in the graph represents a task which is a set of instructions that must be executed serially in the same processor, associating with its computation cost. Additionally, task executions are assumed to be nonpreemptive. The edges in the graph correspond to the communication messages and precedence constraints among the nodes. The source node and the

*National Natural Science Foundation (Grant NO.60534060);
*Shanghai Science & Technology Research Plan (Grant NO.06JC14065).

destination node of an edge are called the predecessor node and the successor node respectively. In a task graph, a node which does not have any predecessor is called an *entry* node while a node which does not have any successor is called an *exit* node. The heterogeneity has been modeled by assuming the different runtime of tasks on different processors. The DAG is $G=\{V,E,r,d\}$, where V is the set of task nodes and E is the set of communication edges.

$V=\{v_i; i\in[1,N]\}$ is the set of task.

$$r(i,u)=\frac{program_i}{S_u} \quad (1)$$

denotes the run time of task v_i on processor p_u.

The average run time of task v_i is defined as

$$\bar{r_i}=\frac{1}{M}\sum_{j=1}^{M} r(i,j) \quad (2)$$

$E=\{e(i,j); i,j\in[1,N], e(i,j)\in[0,1]\}$ denotes the partial order between v_i and v_j.

$d=\{d(i,j); i,j\in[1,M]\}$ denotes the communication cost between v_i and v_j.

$$d(i,j)=lm_u+\frac{data_{i,j}}{B_{u,v}} \quad (3)$$

where task v_i on processor p_u and task v_j on processor p_v.

A Critical Path (CP) of DAG is a set of nodes and edges, forming a path from an *entry* node to an *exit* node, of which the sum of computation costs and communication costs is the maximum. The length of the critical path is the number of nodes on the longest path from *entry* to *exit*. The following notation will be used:

$C=\{c_i; i\in[1,T]\}$ is the set of path from the *entry* to *exit*.

$L(C)$ is the execution time of path C.

$l(C)$ denotes the number of nodes on the path C.

The objective of scheduling is to minimize the schedule length by properly allocating the nodes of DAG to *PE* and sequencing their start-time so that the precedence constraints are preserved. The scheduling result can be obtained by minimize the execution time of the path of DAG from the *entry* to *exit*.

$$Ts=\min_{1\le u\le M}\{\max_{1\le s\le T} L(C_s,P_u)\} \quad (4)$$

The execution time of the longest path can be expressed as the sum of the computation time and the waiting time of the tasks on the path.

$$L(C_s,P_u)=\sum_{i=1}^{l(C_s)}(r(C_i,P_u)+w(C_i,P_u)) \quad (5)$$

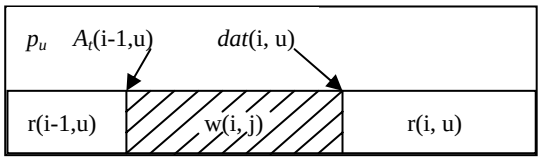


Fig.1 Scheduling task i on processor p_u

The waiting time of task C_i on processor P_u is expressed as

$$w(i,P_u)=dat(i,P_u)\sim A_t(i-1,P_u) \quad (6)$$

where $a\sim b=\begin{cases}a-b, & a>b\\ 0, & otherwise\end{cases}$.

The date arrive time of task C_i on processor P_u is the maximum sum of C_i's predecessor tasks finish time and communication time.

$$dat(i,P_u)=\max_{\substack{k\in prec(i)\\ 1\le v\le p}}\{Ft(k,v)+d(k,i)\} \quad (7)$$

According to the above analysis, we get the following the conclusions:

(1) To reduce the schedule length, we need to minimize the execution time of the longest path of DAG.

(2) The runtime of a task on the processor includes two parts: the computation time and waiting time. The waiting time depends on the finish time of the predecessor task and communication cost between them.

3. DCPD ALGORITHM

The longest path of DAG is the critical path which determines the partial schedule length. Thus, the nodes on the CP have to be scheduled properly in time and space. However, as the scheduling process proceeds, the CP can change dynamically. That is, a node on the CP at one step may be not at the next step. This is because the communication cost among two nodes is considered zero if the nodes are scheduled to the same processor. In order to distinguish the CP at an intermediate scheduling step from the original CP in the task graph, we call it the dynamic critical path (DCP). To reduce the scheduled length, we need to assign the nodes on DCP to the suitable processors and reduce the waiting time for them by clustering or duplicating. A new algorithm DCPD is provided by duplicating the nodes on dynamic critical path in this paper. Before introducing the details, we discuss the parameters for it.

3.1 Parameter of DAG

To identify the nodes on the DCP, we introduce two attributes for each node. The earliest start time (*EST*) for task n_j on processor p_v is defined by

$$est(j,v)=\max_{\substack{i\in PRED(j)\\ 1\le u\le T}}\{est(i,u)+r(i,u)+w(i,j)c_{i,j}\} \quad (8)$$

where $w(i,j)=\begin{cases}1, & u=v\\ 0, & otherwise\end{cases}$ and $PRED(j)$ is the set of immediate predecessor of task n_j.The *EST* is computed recursively by traversing the task graph downward from the *entry* task, and $est(n_{entry})=0$. The dynamic critical path length, denoted by $Max\{est(j,v)+\bar{r_j}\}$.The value of the DCPL is simply the schedule length of the partially scheduled task graph. The latest start time (*LST*) for task n_i is defined by

$$lst(i,u)=\min_{\substack{i\in SUCC(j)\\ 1\le v\le T}}\{lst(j,v)-w(i,j)c_{i,j}-r(i,u)\} \quad (9)$$

where $SUCC(j)$ is the set of immediate successors of task n_i. The *LST* is computed recursively by traversing the task graph upward from the *exit* task of the graph, and $lst(n_{exit})=DCPL-\overline{r_{exit}}$. The very important predecessor of task n_i ($vip(n_i)$) is the one which offers the $Max\{ect(i,u)+c_{i,j}\}$, where $ect(i,u)=est(i,u)+r(i,u)$. Similarly, the very important successor of task n_i ($vis(n_i)$) is the one which offers the $Max\{ect(i,u)+c_{i,j}+\bar{r_j}\}$. The

favorite processor of n_i ($f_p(n_i)$) is the processor which offers the $min\{r(i,u)\}$.

THEOREM 1: If $est(i,u) = lst(i,u)$, then n_i is a node on the DCP.

PROOF: Assume on the contrary that n_i is not on the DCP, the path with the largest sum of computation costs and communication costs, from n_{entry} to n_{exit} , leaping over n_i , which length is DCPL. Then, by the definitions of EST and LST, $est(i,u)$ is equal to the sum of computation costs and communication costs from n_{entry} to n_i , excluding $r(i,u)$; and $lst(i,u)$ is equal to the sum of computation costs and communication costs from n_i to n_{exit} , which can also be expressed as $DCPL - max\{\sum_{entry}^{exit}(\overline{w_i} + d_{i,j})\}$. According to the assumption $est(i,u) + lst(i,u) < DCPL$, this in turn implies that $est(i,u) \neq lst(i,u)$ .Thus, n_i is on the DCP.

3.2 The Insert Rule

The DCPD algorithm uses an insertion based strategy which considers the possible insertion of a task in an earliest idle time slot between two already scheduled tasks on a processor. A node n_i can be assigned to processor p_u , on which a set of m nodes $\{n_1, n_2 ... n_m\}$ have been scheduled, if there exists some value of *k* such that:

$$Min\{lst(i,u) + r(i,u), lst(k+1,u)\} - Max\{est(i,u), est(k,u) + r(k,u)\} \geq w(i,u)$$

Where k=0,1,...m , $lst(m+1,u) = \infty$, and $est(0,u) = 0$.

After n_i is inserted into a processor, the communication cost among the nodes on the processor are set to zero. In addition, to preserve the linearity, a zero cost edge is added from the preceding node to n_i , and another zero cost edge is added from n_i to the succeeding node. Thus, n_i 's *EST* and *LST* on processor p_u can change due to the linear ordering of the nodes according to the start time within the processor.

3.3 DCPD Algorithm

An accurate determination of important nodes for duplication is the key to obtain a short makespan. The most important nodes are those on the critical path, and their finish time determines the final schedule length. Thus the nodes on the CP should be examined for scheduling on the processors which provide the minimize runtime. However, the critical path varies during the scheduling process, so the nodes on the dynamic critical path are of vital importance. Inserting them on the proper time slot or duplicating their important predecessors on the most suitable processor depends on which will reduce the complete time for them. Meanwhile the looking forward policy should also be used and their important successor should be taken into account. As to those unimportant nodes, assign them to the processors which will not increase the whole makespan.

```
Schedule (Ta,Pr );
{
  1) calculate EST and LST for all node by r̄_i , and set the favorite processor ;
  2) put the nodes on the critical path in the CPset;
  3) select the processor (Pcp) which minimize the sum of runtime for the nodes in the CPset, and update the corresponding f_p ;
  4) while not all nodes scheduled do
  {
  5) n_i :the node with the nodes with the smallest difference between its EST and LST;
  6) if n_i in CPset //case 1
  7) assign n_i on CPC //schedule all CP nodes on Pcp;
  8) else if n_i has the equal EST and LST //case 2
  9) assign n_i on processor minimum sum of {ect(n_i)+est(VIS(n_i));
  10) else
  11) scheduling the node on the processor which will not increase the makespan; //case 3
  12) update EST, LST, and f_p for all nodes;
  }
}.
```

Fig.2. DCPD Algorithm

The details of scheduling a node of case 2 will be discussed in the following.

Form the $P\_list = \{f_p(n_i), f_p(vip(n_i)), f_p(vis(n_i)), p(hd)\}$

Case 1: $f_p(n_i) = f_p(vip(n_i)) = f_p(vis(n_i))$

$ect(n_i) = ect(n_i, f_p(n_i))$ //insert n_i on $f_p(n_i)$

$est(vis(n_i)) = ect(n_i)$

Case 2: $f_p(n_i) = f_p(vip(n_i))$

$ect(n_i) = ect(n_i, f_p(n_i))$

$est(vis(n_i)) = ect(n_i) + d(n_i, vis(n_i))$

Case 3: $f_p(vip(n_i)) = f_p(vis(n_i))$

$ect(n_i) = ect(vip(n_i), f_p(n_i)) + r(n_i, f_p(n_i))$

//duplicate $vip(n_i)$ to minimize the earliest complete time

$est(vis(n_i)) = ect(n_i)$

Case 4: $f_p(n_i) \neq f_p(vip(n_i)) \neq f_p(vis(n_i))$

$ect(n_i) = ect(vip(n_i), f_p(n_i)) + r(n_i, f_p(n_i))$

$est(vis(n_i)) = ect(n_i) + d(n_i, vis(n_i))$

Case 5:

$ect(n_i) = ect(vip(n_i), p(hd)) + r(n_i, p(hd))$

//assign n_i to the lightest workload processor.

$est(vis(n_i)) = ect(n_i) + d(n_i, vis(n_i))$

Calculate the $ect(n_i)$ and $ect(n_i)$ for the above 5 cases, and choose the processor which offers the minimum sum of them.

The first stage, used for calculating the parameters for all nodes, has a time complexity $O(P(N+E))$. The dominant part of the algorithm is the "while" loop. This loop executes $O(N)$ times as there are *N* nodes in the DAG. Only the nodes on the dynamic critical path need consider the 5 different cases. There are $O(logN)$ [7] nodes on the critical path of DAG and $O(logN)$ edges along the critical path. Each time assign these nodes to 4 special processors and compare 5 different cases, trying inserting or duplication strategies. The time complexity is $O(5logN)$ .After assigning the node to the proper processor, the nodes parameters will be updated, and the time complexity is $O(N+E)$. Thus the average overall time complexity is $O(NlogN)$ and the worst case is $O(N^2)$.

4. SIMULATION ON SIMGRID[8]

Simgrid is a toolkit that provides core functionalities for the simulation of distributed applications in heterogeneous distributed environments. Simgrid comes in two flavors.

(1) The first one (SG) is a rather low-level toolkit that provides core functionalities for the simulation of distributed applications in heterogeneous distributed environments. SG is suitable for simulation on DAG scheduling.

(2) The second one (MSG) is a simulator built using the previous toolkit. It aims at being realistic and is more application-oriented.

As the scheduling algorithm is based on DAG, we choose SG as simulator. A simulation on Simgrid usually includes three parts: the topology of resource interconnections, the structure of task graph, and the scheduling strategies. Simgrid treats CPUs and network links as unrelated resources and it does not make any distinction between data transfers and computations: both are seen as tasks. It is the responsibility of the user to ensure that their requirements are met.

4.1 Related Algorithm

Some task scheduling schemes have been provided in recent years, including DLS, HEFT, CPOP, TANH.

(1) Dynamic-Level Scheduling (DLS) Algorithm[5]
This algorithm belongs to the list scheduling scheme. During the scheduling processing, the algorithm chooses the ready node and available processor pair that maximizes the value of dynamic level. The complexity is $O(v^3 p)$.

(2) Heterogeneous-Earliest-Finish-Time Algorithm[2]
It is a two-phase algorithm. The first phase queues the task by non-increasing order of nodes priority. Then select the proper processor. The HEFT algorithm has an insertion-based policy which considers the possible insertion of a task in an earliest idle time slot between two already scheduled tasks on a processor. The complexity of HEFT algorithm is $O(pv^2)$.

(3) The Critical-Path-on-a-Processor Algorithm[2]
Like HEFT algorithm, this algorithm set the computation cost of tasks and communication cost with mean values. During the scheduling process, select the highest priority task n_i from priority queue, if n_i is on the CP, assign it on P_{cp}, otherwise, assign it to the processor p_k that minimize *EFT* for it. The complexity is $O(pe)$.

(4) Task Duplication-Based Scheduling Algorithm[1]
The TANH algorithm has been proved to be optimal for DAG with some restricts. Calculate the earliest start time and the earliest complete time for every node. Queue the favorite processors for each node (*fp*), which yield a minimum completion time for it. Decide the favorite predecessor for the nodes. Compute the latest allowable completion time and latest allowable start time for all nodes in a bottom-up traversal of the DAG. Assign the level for nodes. The algorithm schedules the nodes to the processor, taking the task's *fp* and other parameters into account. The complexity of TANH is $O(v^2)$. The optimality conditions for TANH are very strict, when the DAG is of coarse grain, and the communication requirements must be lower than the computation requirements.

4.2 Task Graph Generation

The simulations on simgrid generate random structure of task graph, including the in tree, out tree, fork join, etc. The computation cost of the individual nodes and the communication cost of the edges are all randomly chosen. Within each type of graph, different values of CCR are used. The communication-to-computation ratio (CCR) of a parallel program is defined as its average communication cost divided by its average computation cost on a given system. The CCR range varies from 0.1 to 10.

4.3 Performance Metric

NSL: Since a large set of task graphs with different properties is used, it is necessary to normalize the schedule length to a lower bound, which is determined by

$$NSL = \frac{makespan}{T_G} \tag{10}$$

Number of occurrence of better quality of schedules: The number of times that each algorithm produced better, worse, and equal quality of schedules.

Running time of the algorithm: It is the execution time of an algorithm for obtaining the output schedule of a given task graph. This metric basically gives the average cost of each algorithm.

4.4 Experiment Result

Task duplication schemes are, in general, observed to be better than the Priority based and Cluster based schemes. The TANH and DCPD algorithm show to outperform the other algorithms for different CCR. For computation intense DAG, DCPD works as well as TANH; as to communication intense DAG, DCPD works better. DLS runs much longer time than the other algorithms. Generally, DCPD needs less time than others. Figure 3~7 illustrate the results.

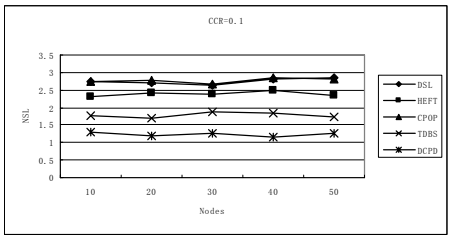


Fig.3 Makespan compare for CCR=0.1

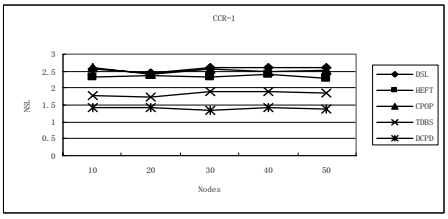


Fig.4 Makespan compare for CCR=1

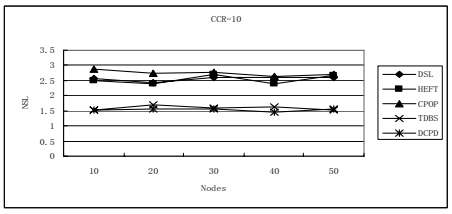


Fig.5 Makespan compare for CCR=10

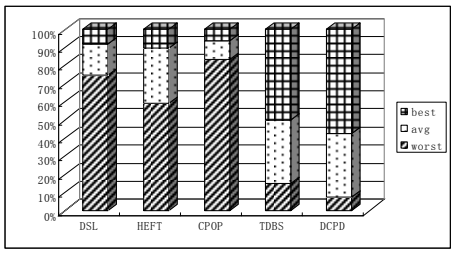


Fig.6 Best, average and worst case compare

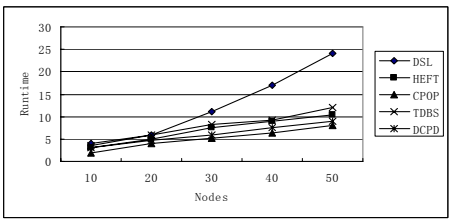


Fig.7 Runtime compare

5. CONCLUSION

To reduce the schedule length, we need to minimize the execution time of the longest path of DAG. As the scheduling process proceeds, the critical paths change dynamically. In this paper, a new algorithm called DCPD is provide for scheduling application task graph onto a system of heterogeneous processors, which schedules the tasks on the dynamic critical path by duplication and looking forward policy to choose the most suitable processors for them. Some simulations have been made on Simgrid. The simulation results show that DCPD outperform them in term of makespan and other metrics.

REFERENCES

[1] Rashmi B, Dharma P, "Improving Scheduling of Tasks in a Heterogeneous Environment", IEEE Trans. on Parallel and Distributed Systems, Vol.15,No.2, February 2004, pp.107~118.

[2] Haluk T, Smlim H, Min-You W, "Performance-Effective and Low-Complexity Task Scheduling for Heterogeneous Computing", IEEE Trans. on Parallel and Distributed Systems, Vol.13,No.3,March 2002,pp.260~273.

[3] Kwok YK, Ahmad I, "Dynamic Critical-Path Scheduling: An Effective Technique for Allocating Task Graphs to Multiprocessors", IEEE Trans. on Parallel and Distributed Systems, vol.7,No.5, March 1996,pp:506~521.

[4] Ishfaq Ahmad, Yu-Kwong Kwok, "On Exploiting Task Duplication in Parallel Program Scheduling", IEEE transaction on parallel and distributed systems, Vol9, No.9,September 1998,pp: 872~892.

[5] Gilbert C S, Edward, A Lee, "A Compile-Time Scheduling Heuristic for Interconnection Constrained Heterogeneous Processor Architectures", IEEE Tran. on Parallel and Distributed Systems, Vol. 4, No.2, February 1993, pp:175~187.

[6] Tracy D. Braun, et al, "A Comparison Study of Static Mapping Heuristics for a Class of Meta-tasks on Heterogeneous Computing Systems", The 8th Heterogeneous Computing Workshop, IEEE Computer Society and office of Naval Research, San Juan, Puerto Rico, April 1999.

[7] Bialek, J, Grey, D.J. "Application of Clustering and Factorization Tree Techniques for Parallel Solution of Sparse Network Equations Generation Transmission and Distribution", IEE Proceedings Vol.144, No.6, 1994, pp:609~ 616.

[8] Simgrid.http://simgrid.gforge.inria.fr.

Fei Yin is a PhD candidate of Computer Software and Theory, Tongji University. Her current research interests include network computing and performance evaluation.

Xiaoli Du is a PhD candidate of Computer Software and Theory, Tongji University. Her current research interests include network computing and parallel algorithm.

Changjun Jiang is a Full Professor and a PhD supervisor. He is now the dean of School of Electronic and Information Engineering in Tongji University. His current research interests include network computing, semantic grid and Petri nets.

Rong Deng is a PhD candidate of Computer Software and Theory, Tongji University. Her current research interests include grid computing and resource management.

A Scheduling Heuristic for Large-Scale Heterogeneous Computing Environments*

Xiao Li Du[1,2], Chang Jun Jiang[2,3], Fei Yin[1,2]
[1]Electronics and Information Engineering School, Tongji University
Shanghai, 201804, China
[2]Tonji Branch, National Engineering &Technology Center of High Performance Computer
Shanghai, 201804, China
[3]Key Laboratory of Computer System and Architecture, Institute of Computing Technology, Chinese Academy of Sciences
Beijing, 100080, China
Email: du_xiaoli@163.com

ABSTRACT

A group of features is defined to describe the synthetic performance of processing cells and distinguish their heterogeneousness in large-scale heterogeneous computing environments. Three notable features that can effectively partition the processing cells of target system with fuzzy clustering are verified through several groups of experiments. Based on fuzzy clustering results of the target system, a Scheduling heuristic algorithm is presented. In the scheduling stage, the cluster with better synthetic performance will be chose first. The algorithm greatly reduces the time spent on the processor selection for large-scale system. The priority designation of tasks takes the influence of critical path nodes and heterogeneous resource into consideration. Experimental results show that it performs very well compared with other algorithm.

Keywords: Task Scheduling, Heterogeneous Computing, Direct Acyclic Graph

1. INTRODUCTION

How to schedule a program onto a multiprocessor system to minimize the program completion time is a well-known problem in parallel computing and processing. In general, finding an optimal schedule is an NP-complete problem, so researchers have resorted to devising efficient heuristics. Many early task scheduling algorithms made simplifying assumptions about the parallel program and target system, such as uniform task execution times, zero inter-task communication times, uniform processor execution rate and messages passing rate. Some researches about heterogeneous computing mainly concern the problem of independent task scheduling. Some algorithms considering temporal dependencies among tasks suppose communication links with uniform transmitting rate or full connectivity of parallel processors. Presently, most scheduling algorithms are designed under the assumption of homogeneous computing environments, such as, list scheduling [1~2], task-duplication based scheduling algorithm[3~4], task clustering based scheduling algorithm[5~6], modern optimization approaches like genetic algorithms, randomization approaches etc. Most task scheduling algorithms under heterogeneous computing environments suppose that there doesn't have inter-task communication, such as Max-min and Min-min. With the rapid development of network technique, heterogeneous computing (HC) has become the future research direction. HC will make it possible to solve complicated problems through geographically distributed processors interconnected by high-speed network. Therefore, task scheduling for heterogeneous computing will be a new hotspot of the research filed.

In large-scale heterogeneous computing environments, exist tremendous processing cells geographically distributed, and result stupendous cost of choosing the fit processing cell during the scheduling process. This paper presents a group of features that can synthetically describe the performance of processor. Then, every processing cell has a pattern vector, which distinguishes it from others. Here, the heterogeneousness mainly refers to different processing cells with different execution rate and link broad width. The fuzzy clustering of the target system can be thought as a pretreatment that would largely reduce the time cost of choosing processors during the scheduling process. Furthermore, a fuzzy clustering based scheduling heuristic (FCBSH) is presented, which takes both the resource heterogeneousness and temporal dependencies among tasks into amount. It also tries to reduce every task's completion time at every step so as to reduce the completion time of the entire program.

The rest parts of this paper are organized as follows: Section 2 introduces the preliminary definitions and notations. Section 3 presents the fuzzy clustering of target system. Section 4 is devoted to the FCBSH algorithm formulation. Section 5 shows experimental results and performance analyses. Section 6 summarizes this discussion.

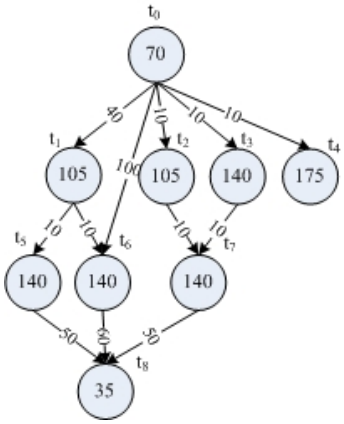


Fig.1. Task graph [7]

2. PRELIMINARY DEFINITIONS AND NOTATIONS

2.1 Task Graph

* Supported by the National Natural Science Foundation of China under Grant No. 60534060; the 2006 Mountaineering Program of Science & Technology Committee of Shanghai under grant No. 06JC14065.

A task graph is a directed acyclic graph (DAG) G= (V_g, E_g), where V_g is a set of nodes and E_g is a set of directed edges. A node in the DAG represents a task denoted by t_i, and the weight of t_i is its computation requirement presented by $W(t_i)$. N_g=$|V_g|$ is the amount of nodes and Ne_g=$|E_g|$ the amount of edges. The directed edge in the DAG, denoted by (n_i,n_j), and weights by C(n_i,n_j) represents the communication requirement of the edge. If n_i and n_j are allocated onto the same processor, then C(n_i,n_j) is zero. A task cannot start its computation before receiving all communication messages from every predecessor node. $PRED$(n_x) denotes the predecessor node set of n_x, and $SUCC$(n_x) is the successor node set. It is supposed that every task can be executed on any processor of the target system. An example of DAG is shown in Fig.1.

The scheduled nodes (SN) are the nodes have been allocated on processors. The unscheduled nodes (USN) represent the nodes have not been allocated. Ready nodes (RN) are a set of nodes whose predecessor nodes have finished computation. If $n_i \in USN \cap RN$, then $PRED(n_i) \in SN$. $BL(n_x)$, also called Bottom-Level, is the length of a longest path from n_x to an exit node. In general, scheduling in a descending order of b-level tends to schedule critical path nodes first. Under heterogeneous computing environments, processors have various execution rates and communication links with different message passing capability, therefore, the median of execution rate over all processors, donated by Mp, and the median of message passing capability of all communication links, represented by Mc, are used to scale the node precedence under heterogeneous computing, donated by BL*.

$$BL^*(t_i) = W(t_i)/M_p + \max_{t_j \in SUCC(t_i)} (C(t_i,t_j))/M_c + BL^*(t_j)) \quad (1)$$

The actual start time of t_i on processor p_j is denoted by $ST_{p_j}(t_i)$, and the finished time of t_i on processor p_j presented by as follows.

$$FT_{p_j}(t_i) = ST_{p_j}(t_i) + W(t_i)/W(p_j) \quad (2)$$

Suppose $t_i \in PRED(t_j)$ is allocated to p_x, and t_j to p_y. If x=y, then $C(t_i,t_j) = 0$. The arriving time of messages from t_i to t_j is shown as follows.

$$AT_{p_y}(t_i,t_j) = FT_{p_x}(t_i) + C(t_i,t_j)/C(p_x,p_y) \quad (3)$$

Then, the earliest start time of t_j on processor p_y is presented as follows.

$$EST_{p_y}(t_j) = Max\{\max_{t_i \in PRED(t_j) \cap SN}\{AT_{p_y}(t_i,t_j)\}, FT_{p_y}(t_q)\} \quad (4)$$

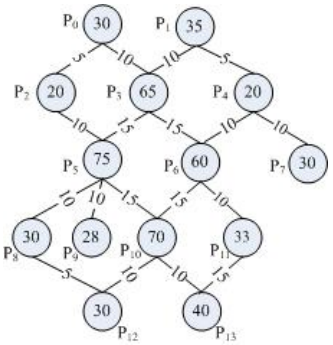


Fig.2. Target system

2.2. Target System

The target system, donated by P=(V_P,E_P) is assumed to be a network of processing cells. Each processing cell has a local memory unit so that the processing cell doesn't share memory and communication relies solely on message-passing. Where, VP is the set of processors and E_P the set of edges (links). N_p=$|V_P|$ and N_{ep} =$|E_P|$ represent the amount of processors and links respectively. C(p_i,p_j), the weight of link (p_i,p_j), is the time cost spent on passing one unit of message. The weight of the node, donated by W(p_i), represents the amount of computation that can be performed by the processing cell in a time unit. See an example shown in Fig.2.

3. FUZZY CLUSTERING OF THE TARGET SYSTEM

The heterogeneous computing environments in this paper mainly refer to the different computation capacities among processing cells and different communication capacities among links. It is obvious that how to choose processing cell for tasks would influence the completion time of their successors and even the entire program. Because of the heterogeneousness, it needs to find the suitable features to screen the heterogeneousness and evaluate the performance of the processing cell synthetically. Because there does not have strict feature differences among processing cells, it suits to do soft partition, which is also called fuzzy clustering.

3.1 Feature Definition

Undoubtedly, the primary problem presented to us, is how to define, choose the features that describe processing cells in target system. Firstly, we try to find out all features that can depict the heterogeneousness including computation and communication capacity of processing cells. Secondly, choose the notable features that could reasonably partition the target system. For the first step, our former research [8] only presented five features and did not address this problem in detail. In this paper, seven features are found out through our further research, and the notable features are verified in 3.2.

(1) Processing Capacity (PC): $PC = W(p_i)$ the amount of computation that can be performed by the processing cell in a time unit.

(2) The Average Communication Capacity (ACC): $ACC = \sum_{j \in Nei(i)} C(p_i,p_j) / n$, the average communication capacity of links connected with the processing cell. Where, Nei(i) is the set of adjacent nodes of i.

(3) The Neighbor Average Processing Capability (NAPC): $NAPC = \sum_{j \in Nei(i)} W(p_j) / n$, the average processing capability of the nodes in Nei(i).

(4) The Network Location (NL): $NL = n \cdot \max_{j \in V_p, j \neq i} \{ShortPath(i,j)\}$, the processing cell's location in the target system, the smaller the NL is, the closer the processing cell comes to the network center of the target system or to the margin in contrast. Where, $\max_{j \in V_p, j \neq i} \{ShortPath(i,j)\}$, is the maximum hops from i to every processing cell in the target system. n is the amount of the processing cells that have the maximum hops to i.

(5) The Minimum Communication Capacity (MICC): $MICC = \min_{j \in Nei(i)} \{C(p_i,p_j)\}$, the minimum communication capacity among links connected with i.

(6) The Amount of Links (AL): the amount of links connected with the processing cell.

(7) The Maximum Communication Capacity (MCC): $MACC = \max_{j \in Nei(i)} \{C(p_i,p_j)\}$ the maximum communication

capacity among links connected with *i*.

In the above definitions of the seven features, PC reflects the computation speed of the processing cell itself, while NAPC represents the processing cell's neighborhood computation speed. That is to say choose a processing cell with better NAPC will better the execution of its subsequent nodes. The rest five features denote the communication capacity of links connected with the processing cell in a certain way. Well then, which are the notable features that can partition the target system reasonably?

3.2 Fuzzy Clustering

Each processing cell $p_k \in V_p$ has a pattern vector denoted by $P(p_k)=(p_{k0},p_{k1},\ldots,p_{ks})$. Where, p_{kj} (j=0,2,…,s) presents the j[th] feature of the p_k, and $s \in [3,7]$ is a positive integer. Then we get the feature vector matrix. However, the data in table.1 are not in the range [0, 1], range standardization method is applied to standardize these data and shown in Equ.(5) and Equ.(6).

$$p'_{ik} = (p_{ik} - \bar{t}_k) \Big/ S_{t_k} \quad (5)$$

Where, $\bar{t}_k$ is the average of the k[th] dimension feature t_k in table.1, and S_{t_k} is the standard deviation of t_k.

$$p''_{ik} = (p'_{ik} - p'_{k\,min}) \Big/ (p'_{k\,max} - p'_{k\,min}) \quad (6)$$

Where, $p'_{k\min} = \min_{0 \le j \le N_p - 1} \{p'_{jk}\}\, p'_k$, and $p'_{k\max} = \max_{0 \le j \le N_p - 1} \{p'_{jk}\}$

Thereafter, a simulation relation matrix of processing cells in target system, donated by $\tilde{R}_s$, is obtained through exponent similarity coefficient method. Furthermore, the fuzzy equivalence matrix with transitive closure, represented by $\tilde{R}_e$, is calculated by performing matrix resultant operation on $\tilde{R}_s$. Finally, the fuzzy clustering results can be acquired through setting the value of α-level cut. If the value of α approaches 1, the fuzzy clusters obtained above are more similar. Contrarily, if it is close to zero, the similarity among the fuzzy clusters is worse. After obtaining the fuzzy clusters, the synthetic performance of each cluster can be calculated by the following equation.

$$PERF(CL_j) = \frac{1}{n} \sum_{p_k \in CL_j} \sum_{i=0}^{s-1} \alpha_i * P''[k][i] \quad (7)$$

Where, n is the amount of the clusters in the clustering result, and CL_j is the j[th] cluster. α_i is the weight of the i[th] feature of the processing cell.

3.3 Notable Feature Selection

Table 1. Feature vector matrix of the five groups

	t_0	t_1	t_2	t_3	t_4	t_5	t_6
p_0	30.00	7.50	42.50	12.00	5.00	2.00	10.00
p_1	35.00	7.50	42.50	8.00	5.00	2.00	10.00
p_2	20.00	7.50	52.50	5.00	5.00	2.00	10.00
p_3	65.00	12.50	50.00	9.00	10.00	4.00	15.00
p_4	20.00	8.33	41.67	12.00	5.00	3.00	10.00
p_5	75.00	12.00	42.60	4.00	10.00	5.00	15.00
p_6	60.00	12.50	47.00	9.00	10.00	4.00	15.00
p_7	30.00	10.00	20.00	15.00	10.00	1.00	10.00
p_8	30.00	7.50	52.50	5.00	5.00	2.00	10.00
p_9	28.00	10.00	75.00	5.00	10.00	1.00	10.00
p_{10}	70.00	12.50	51.25	9.00	10.00	4.00	15.00
p_{11}	33.00	12.50	50.00	12.00	10.00	2.00	15.00
p_{12}	30.00	7.50	50.00	12.00	5.00	2.00	10.00
p_{13}	40.00	12.50	51.50	12.00	10.00	2.00	15.00

With Fig.2, five groups of experiments are performed to find the notable features. The pattern vector using in the first group contains all seven features, and reduces one in turn in the rest four groups. According to 3.2, we get the feature vector matrix of every group seen in table1. The entire table1 is the feature vector matrix of the first group and the three gray-black columns is that of the fifth group. The fuzzy clustering results the five group experiments are shown in table2. It is easy to see that there is little difference among the results of five groups. The fifth experiment only uses three features, however, the only difference between the fifth experiment and the rest four is {3,5,6,10} in fifth experiment but {5} and {3,6,10}in other four experiments. Furthermore, the ranked results according to Equ.(7) of the five groups also have little difference.

Table 2. The fuzzy clustering results of five groups

Group	Pattern vector	Clustering results	Ranked results
1	(PC,ACC,NAPC, NL, MICC, AL, MACC)	{{0,1,2,4,8,12},{3,6,10},{5},{7},{9},{11,13}}	{{5},{3,6,10},{11,13},{9},{0,1,2,4,8,12},{7}}
2	(PC,ACC,NAPC, NL, MICC, AL)	{{0,1,2,4,8,12},{3,6,10},{5},{7},{9},{11,13}}	{{5},{3,6,10},{11,13},{9},{0,1,2,4,8,12},{7}}
3	(PC,ACC,NAPC, NL, MICC)	{{0,1,2,4,8,12},{3,6,10},{5},{7},{9},{11,13}}	{{5},{3,6,10},{11,13},{9},{0,1,2,4,8,12},{7}}
4	(PC,ACC,NAPC, NL)	{{0,1,2,8},{4,12},{3,6,10},{5},{7},{9},{11,13}}	{{5},{3,6,10},{11,13},{9},{4,12},{0,1,2,8},{7}}
5	(PC,ACC,NAPC)	{{0,1,2,4,8,12},{3,5,6,10},{7},{9},{11,13}}	{{3,5,6,10},{11,13},{9},{0,1,2,4,8,12},{7}}

Table 3. Clustering results of random generated target systems

(PC,ACC,NAPC, NL,MICC,AL, MACC)	(PC,ACC,NAPC,NL, MICC, AL)	(PC,ACC,NAPC)
{{0},{1},{2},{3},{4,5,8},{6},{7},{9,10,11,13}, {12}, {14}}	{{0},{1},{2},{3},{4,5},{6},{7},{8},{9,10,11,13,14}, {12}}	{{0,1},{3,7},{4},{5,6},{8},{2,9,10,11,13,14},{12}}
{{4,5},{1},{7},{6},{11},{2},{8},{10},{14},{11,13}, {3},{0},{9}}	{{4,5},{7},{1},{2},{10},{11},{6},{12,13,14},{3},{0},{8},{9}}	{{5},{1,6},{0,2,4,7,10},{3},{11,12,13,14},{9}}
{{0},{1,2,5},{3},{4},{6},{7},{8,9}}	{{0},{1,2,5},{3},{4},{6},{7},{8,9}}	{0,3},{1,2,5},{4},{6,7}{8,9}
{{0,1,7,8,9},{2},{3},{4},{5}, {6}}	{0,1,7,8,9},{2},{3},{4}, {5},{6}	{0,1,6,7,8,9},{2},{3,4},{5}
{{0,2,7,12,13,14,16,18,},{1},{3,4,6,9,10},{5},{8},{11},{15},{17}, {19}}	{{0,2,7,12,13,14,15,16,17,18,19,},{1},{3},{4,6,9},{5},{8},{10},{11}}	{{0,2,7,8,12,13,14,15,16,17,18,19},{1},{3},{6,4,9},{5},{10},{11}}
{{0,3,4,5,6,7,13,14,15,16,17,18,19},{1},{2},{8,9,11},{10},{12}}	{{0,3,5,6,7,13,14,15,16,17,18,19},{1},{2,12},{4},{8,9,10, 11}}	{{0,2,3,5,6,7,12,13,14,15,16,17,18,19},{1},{4},{8,9},{10,11}}

Utilizing the random target system generator [8], a group of target systems with 10, 15, and 20 nodes are generated. Choosing the pattern vector in the first, third, and fifth group of the above experiment, the randomly generated target systems are fuzzily clustered and their results are shown in table 3. From table 3, we can see the fuzzy clustering results of experiment with pattern vector (PC, ACC, NAPC) has coarser granularity than experiments with pattern vector (PC, ACC, NAPC, NL, MICC, AL, MACC) and（PC, ACC, NAPC, NL, MICC）, but it realizes the reasonable partitions of the target systems. Moreover, Fig.3 shows it only spends one fifth to one tenth of the cost of experiments with pattern vector (PC, ACC, NAPC, NL, MICC, AL, MACC) and（PC, ACC, NAPC, NL, MICC）.

4. FCBSH ALGORITHM

Obviously, if we can try our best to reduce the completion time of each task, it would be possible to shorten the entire program's make span. The completion time of a task is determined by two factors. One is the start time of the task, the

other one is the execution time. The completion time of predecessors of the current task, messages passing capacities between the processing cells where predecessors locate and the processing cell where the current task is allocated and the completion time of former tasks scheduled on the same processing cell with the current task would influence the start time of the current task. Therefore, how to select processing cells for tasks will be an important influence on the completion time of successors' execution. With the fuzzy clustering work done in section 3, it is easy to choose a processing cell with nice synthetic performance and minimum completion time.

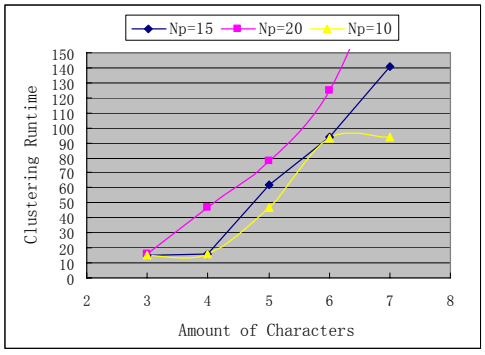


Fig.3. Clustering runtime comparison

The priority of a task is defined as follows.

$$\mathrm{P}riority(t_i) = BL^* + \Delta(Considered, t_i) \quad (8)$$

$$\Delta(Considered, t_i) = \max FTinCon(t_i) - \min FTinCon(t_i) \quad (9)$$

As mentioned above, BL* is calculated by the median of message passing capability over all links and the median of computation capacity. Scheduling in a descending order of BL* tends to schedule critical path nodes first. That is because critical path nodes determine the completion time of the whole program in a certain way. Table 4 shows BL* of tasks in Fig.1. *Considered* is a set of candidate processing cells that are waiting for be selected for tasks. Its initial value is the cluster obtained in section 3 with best synthetic performance. max*FTinCon*(t_i) is the maximum completion time of task t_i obtained from allocating it to processors in set *Considered*. On the contrary, min*FTinCon*(t_i) is the minimum completion time of t_i. The bigger Δ(*Considered*, t_i) is, the more different the completion time of t_i allocated to different processing cells in the set *Considered* is. The task with bigger Δ(*Considered*, t_i) should be assigned higher priority so that it can be allocated to the processing cell providing minimum completion time. If the value of Δ(*Considered*, t_i) is small, it indicates that there is no much difference of completion time among processing cells on which t_i is to be scheduled. So this case has smaller influence on the completion time of entire program.

Table 4. The task BL* of the task graph in Fig.1

Node	*n_0	n_1	n_2	n_3	n_4	n_5	*n_6	n_7	*n_8
BL*	23	15	14	15	5	10	11	10	1

The FCBSH algorithm shown in Fig.4 works as follows.

(1) First perform the fuzzy clustering process on target system according to section 3 and choose the proper α-level cut to obtain the fuzzy clusters of processors.

(2) Put the processing cells in the cluster with best synthetic performance into the set *Considered*.
Repeat

(3) If there exist idle processing sells in *Considered*, compute the priority of each ready node. Schedule the task with highest priority to the processing sell providing the minimum completion time. If there has no idle processing cell in *Considered* and the scheduling of the current task results in the increase of make span, find the best synthetic performance cluster in the rest clusters and select a processing cell in that cluster having the shortest distance to the processing cell with the heaviest load in *Considered*. Calculate the completion time of the current task on the new selected processing cell. If the completion time of the new selected processing cell is smaller than that obtained from the processing cell in Considered, allocate the current task to the new selected one and add the new selected into *Considered*. Otherwise, allocate the current task to the processing cell with the minimum completion time in *Considered*. If two processing cells have the same completion time, choose the one with network location closer to the network center.

(4) Delete the node from *RN* and update *RN*.
Until all tasks in the Task Graph are scheduled.

```
1. Fuzzily cluster the target system, choose the proper α-level cut and
get the fuzzy clusters of processing cells in the target system.
2. Put the processing cells in the cluster with best synthetic
performance into Considered.
3. Let makeSpan=0;
4. Repeat
5. if ( ∃ idle processing cells ∈ Considered)
6.       Let maxPri=0, task=0;
7.      For each t_i∈RN
8.           compute Priority(t_i);
9.           if (Priority(t_i)>maxPri)
10.              maxPri = Priority(t_i);
11.              task = t_i;
12.          endif.
13.     endfor.
14. Schedule task onto the processing cell denoted by p with the
minimum completion time
// If two processing cells have the same completion time, choose the
one with network location closer to the network center.
15.      makeSpan = FT_p (task);
16. else
17.       do step 7-13, find task with the maximum priority;
18.       if (FT_p(task)<= makeSpan)
19.           Schedule task onto the processing cell denoted by p with
the minimum completion time;
20.       else
21.           find the best synthetic performance cluster in the rest
clusters and select a processing cell denoted by p' in that cluster
having the shortest distance to the processing cell with the heaviest
load in Considered;
22.           if (FT_p (task)>FT_p' (task))
23.               allocate task onto p';
24.               add p' into Considered;
25.               makeSpan = FT_p' (task);
26.           else
27.               schedule task onto p;
28.               makeSpan = FT_p (task);
29.           endif.
30.       endif.
31. endif.
32. remove task from RN;
33. update the RN;
34. Until each t_i∈V_t has been allocated.
```

Fig.4. The FCBSH algorithm

5. EXPERIMENT AND PERFORMANCE ANALYSES

The DLS algorithm has certain similar assumptions with our work. So with the task graph and target system randomly generated, three types of experiments are performed to compare the performance between FCBSH and DLS algorithm. First, task graphs with N_g =5 generated randomly are scheduled onto target systems with N_p from 5 to 100. The experiment results in Fig.5 show that the runtime of DLS soars rapidly as the size of target systems scales up, and exceeds 2000 time units when N_p equals to 100. However, the runtime of FCBSH nearly approaches to zero when N_p is less than 70 and is less than 15 time units while N_p is less than 100 but more than 70.

Moreover, we perform 9 groups of experiments with 50 times tests in each group in order to compare the schedule results between FCBSH and DLS. Fig.6 shows the FCBSH results generated in each group better than that of DLS are from 10 to

30 percent, little worse than that of DLS are from 25 to 55 percent, much worse than that of DLS are from 5 to 20 percent and as well as that of DLS are from 20 to 60 percent. Here, "little worse" means that the discrepancies between the results generated by FCBSH and those of DLS are less than 4 time units. "Much worse" means that those discrepancies are more than 4 time units. At last, we compare the performance among FCBSH, DLS and an algorithm denoted by NC that doesn't consider the communication costs among tasks. Fig.7 shows the make span of FCBSH is as well as that of DLS, but less than that of NC. And readers can refer the performance analysis in detail in [8].

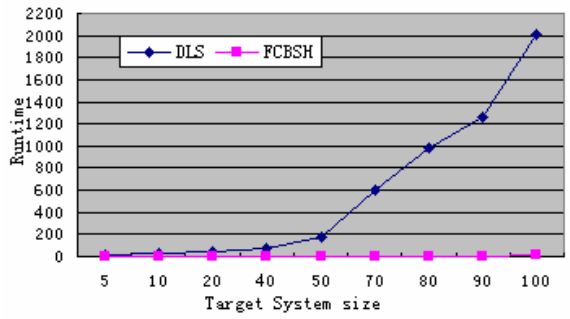


Fig.5 The runtime comparison between DLS and FCBSH

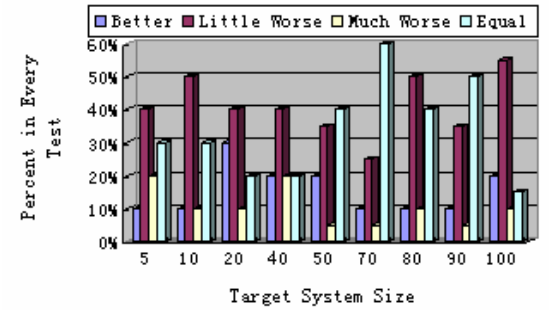


Fig.6 The percent that FCBSH produces better, little worse, much worse and equal results than the DLS does

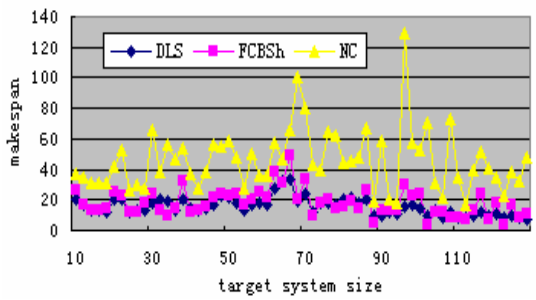


Fig.7. the comparison of make span among FCBSH, DLS and NC algorithm

6. CONCLUSIONS

Focusing on the problem of task scheduling under the large scale heterogeneous computing environment, the main work of this paper has two aspects. Firstly, it presents a group of features describing the synthetic performance of processors and obtains the notable features from experiments and detailed analysis. Based on the clusters generated from fuzzy clustering of the target system, it greatly reduces the time spent on the processor selection. Secondly, a fuzzy clustering based scheduling heuristic is proposed and compared with DLS. And experiments show the runtime of FCBSH are much less than that of DLS with the growth of problem size.

REFERENCES

[1] T L Adam, KM Chandy, J Dickson. "A Comparison of List Scheduling for Parallel Processing Systems," Volume 17. *Communications of the ACM* (1974) 685-690.

[2] GC Sih, E A Lee. "A Compile-time Scheduling Heuristic for Interconnection Constrained Heterogeneous Processor Architectures," Volume 2, *IEEE Transactions on Parallel and Distributed Systems* (1993)75-87.

[3] Y K Kwok, I Ahmad. "Static Scheduling Algorithms for Allocating Directed Task Graphs to Multiprocessors," Volume 31, *ACM Computing Surveys* (1989) 406-471.

[4] I Ahmad, Y K Kwok. "On Exploiting Task Duplication in Parallel Programs Scheduling," Volume 9. *IEEE Transactions on Parallel and Distributed Systems* (1998) 872-892.

[5] V Sarkar. *Partitioning and Scheduling Parallel Programs for Multiprocessors*. MIT Press, Cambridge, MA (1989)90-102.

[6] T Yang, A Gerasoulis. "DSC: Scheduling Parallel Tasks on an Unbounded Number of Processors," Volume 5.*IEEE Transactions on Parallel and Distributed Systems* (1994) 951-967.

[7] YU-KWONG KWOK, ISHFAQ AHMAD. "Static scheduling algorithms for allocating directed task graphs to multiprocessors," *ACM Computing Surveys*, New York: ACM Press, 1999, 31(4): 406-471

[8] DU Xiao-Li, JIANG Chang-Jun, XU Guo-Rong, DING Zhi-Jun. "A Grid DAG Scheduling Algorithm Based on Fuzzy Clustering," *JOURNAL OF SOFTWARE*,2006 Vol.17 No.11 P.2277-2288

Xiaoli Du is a Ph.D candidate of Computer Software and Theory, Tongji University. Her current research interests include network computing and parallel algorithm.

ChangJun Jiang, a professor and Ph.D supervisor is now the dean of School of Electronic and Information Engineering in Tongji University. His current research interests include network computing, semantic grid and Petri nets.

Fei Yin is a Ph.D candidate of Computer Software and Teory, Tongji University. Her current research interests include parallel program performance analysis and grid computing.

An Adaptive Control-based Feedback Load-shedding Strategy *

Lin Ouyang[1], Qingping Guo[1], Qin Zhou[2], Qiumei Pu[1]
[1]School of Computer Science and Technology, Wuhan University of Technology
Wuhan, Hubei 430063 China
[2]Department of Electrical Engineering, Shanghai Dian Ji University
Shanghai 200240 China
Email: [1]oyl@whut.edu.cn, [2]rainbow.zhou@tom.com, [1]puqm@whut.edu.cn

ABSTRACT

There is a large class of applications that produce high-frequency data continuously in 7 days per week and 24 hours per day. The traditional data processing system can't deal with them efficiently because of the active data pushing and the passive queries. With the purpose of dealing with these data, data stream management systems (DSMS) appeared. For the geographical distribution of data streams, distributed data stream processing systems are studied recently. As an important aspect of distributed data stream management system (DDSMS), load management can balance system load incurred by unpredictable incoming data stream and inappropriate query operators' distribution. Load-shedding acts as an important role in load management of distributed data stream system. In this paper, a control-based feedback load-shedding strategy is proposed to degrade system load. Compared with previous work which concentrates on one metric factor only, it takes four metric factors, such as CPU usage ratio, memory utilization, average length of waiting data queue and data tuple delay, into account to increase system stability and to decrease the loss of query accuracy.

Keywords: Load-shedding, Control Theory, Feedback Control, DDSMS

1. INTRODUCTION

A large class of data-intensive applications that produce high-frequency data updates, such as stock markets, network monitoring, online transaction, sensor applications and pervasive environments, have appeared in the past few years. In these typical applications named data stream applications, data are usually unbounded, continuous, huge in amount, fast arriving, time various and out bursting.

The traditional data processing, which can deal with the snapshot queries perfectly, can not satisfy the requirements of these data stream applications. Till now, a number of Data Stream Management Systems (DSMS), such as Aurora [1], Medusa [2], STREAM [3], TelegraphCQ [4], Borealis [5] and Argus [6], have been developed for the purpose of dealing with these continuous streaming data. In these DSMS, the queries are passive and the data are active. On the contrary, the data are passive and the queries are active in traditional data processing systems. Many applications of DSMS system are under real time constraint on query processing. However, delays in data stream processing are very difficult to control because of the outbursting of data incoming and the unpredictable pattern of resource consumption. Therefore, system overloading is very common in data stream systems, especially in distributed data stream processing systems. In order to implement the load balancing in these systems, many kinds of methods are adopted such as operator distribution or redistribution, operator migration and load-shedding etc.. Usually, the load management system takes advantage of load balancing to degrade the system load.

Including other load management methods, load-shedding is also a very efficient and effective method to implement the real time constraint of these applications by dropping incoming data appropriately especially when the incoming data burst out and can't be processed in time through normal load balancing methods.

2. RELATED WORK

Some work has been done in this area recently. The Aurora system [7] uses Quality of Service (QoS), including a latency graph, a value-based graph and a loss-tolerance graph, to implement load-shedding. In Aurora, three basic questions (when, where and how much data should be dropped) are raised for load-shedding, but it mainly focuses on where instead of when and how much to drop data tuples. In [8], load-shedding strategies for a single continuous query operator on sliding window model are presented. The TelegraphCQ [4] system discusses a load-shedding strategy that takes advantage of a data summary method by using a data classifying algorithm to increase the accuracy of queries. In [9], load-shedding strategies that minimize the loss of accuracy of aggregation queries in DSMS are discussed. In [10], a data triage approach is proposed to exploit synopses of discarded data to increase query accuracy. The LoadStar [11] project discusses semantic load-shedding in a stream mining environment. In [12], a systematic approach that takes advantage of well-established feedback control techniques is proposed. In [13], a QoS adaptation framework that smartly adjusts application QoS and performs admission control-based on the current and historical system status is proposed. In [14], a different method is used that focuses on the memory resource utilization in order to give the data some buffer and avoid using the operator selectivity to guide load-shedding.

As we know, various system resources including CPU, memory, and network bandwidth may become the bottleneck in DDSMS query processing. Most of current research mainly concentrates on the management of CPU cycles or memory utilities and assumes that the other resources are sufficient. However, it is not true in the real world. Sometimes almost all the resources, such as the average length of waiting data queue, data tuple delay etc., should be taken into account in order to increase the accuracy of queries. In this paper, an adaptive control-based feedback load-shedding strategy, in which several factors such as CPU, memory, data queue length and data tuple delay are taken into consideration, is proposed.

* It's sponsored by Hubei Natural Science Foundation. Project Number: 2005ABA227

3. CONTROL-BASED FEEDBACK LOAD-SHEDDING

3.1 Control Theory

Control theory has been in use for a long time in automatic control area. In engineering and mathematics, control theory deals with the behavior of dynamical systems. The desired output of a system is called the reference. When one or more output variables of a system need to follow a certain reference over time, a controller manipulates the inputs to a system to obtain the desired effect on the output of the system.

Feedback control, as an important part of control theory, is the basic mechanism by which systems (either mechanical, electrical, or biological) maintain their equilibrium or homeostasis. Feedback control may be defined as the use of difference signals, determined by comparing the actual values of system variables to their desired values, as a means of controlling a system.

In understanding automatic process control, first it is necessary to fix in mind three important terms associated with any process. These three terms are Controlled Variables, Manipulated Variables and Disturbances.

Controlled Variables or Controlled Quantities, are those streams or conditions that the practitioner wishes to control or maintain at some desired level. They are the performance metric controlled by the system. Examples would be flow rates, levels, pressures, temperatures, compositions, and the like. For each of these controlled variables, the practitioner also establishes some desired value or set point, which usually are named as Performance References, to represent the desired system performance in terms of the controlled variables. The difference between a performance references and the current value of the controlled variables is called an error.

Manipulated Variables or Manipulated Quantities are system attributes that can be dynamically changed by the system to affect the value of the controlled variable. For each controlled variable, there is an associated manipulated variable, or manipulated quantity. In process control this is usually a flowing stream, and, in such cases, the flow rate of the stream is often manipulated through the use of some control valve.

Disturbances enter the process and tend to drive the controlled variables away from their desired set point conditions. The need then is for the automatic control system to adjust the manipulated variables so that the set point value of controlled variables are maintained in spite of the effects of the disturbances. Also, the set point may be changed, and then the manipulated variables will need to be changed to adjust the controlled variables to its new desired value.

A basic feedback control system is shown in Fig. 1. In this basic system, the central idea of feedback control is the feedback control loop, which consists of several components: 1. A plant to be controlled; 2. A monitor measuring the relevant status of plant periodically; 3. The measurements from the monitor are sent to a controller as an output signal. The controller compares the value of the signal with a target value that is set beforehand. The difference between the output signal and the target is called the error. The controller then maps the error to a control action; 4. An actuator adjusts the behavior of the plant based on the control action. By this feedback method, the system can control the output signal in a stable level.

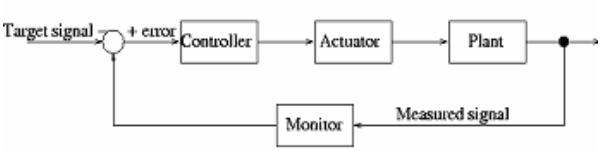


Fig.1. Basic feedback control system

3.2 Adaptive Control-based Feedback Load-shedding Strategy

Previous research work only used single metric variable for load-shedding purpose, and they didn't care about the couple factors as a whole. In this paper, the metric variables, which consist of CPU usage, memory utilization, average length of waiting data queue and data tuple delay, are taken into account to implement adaptive load-shedding.

In our model, we define array variable *CV*, which include memory utilization *M*, CPU utilization *C*, average length of waiting data queue *Q* and data tuple delay *D*, as the controlled variable. All these variable are defined over a time window *{(k-1)W, kW}*, where *W* is the sampling period and k is the the sampling instant. For the simplicity, time window *{(k-1)W, kW}* is also called time window *k*. The controlled variable *CV(k)* denotes the value at the *k*th sampling instant.

Also, we define an array value *PR* that has the same dimension of array *CV*, as performance reference. The difference between a performance reference and the current value of the controlled variable is *E*, and it is calculated by Eq. (1).

$$E(k) = PR - CV(k) \quad (1)$$

Here *E(k)* denotes the total error of *CV(k)*.

In our system, the manipulated variable is data arrival rate *R*. The data arrival rate *R(k)* at the *k*th sampling instant is defined as the average data arrival rate of all data streams at time window k, and it can be measured by recording the average number of data items arriving during this period. *R(k)* is time-varying and not predictable, however, it is assumed that *R(k)* does not vary greatly in two adjacent time windows. This is because the stream data of real-world data stream applications are context-sensitive, which means the change of the state of data stream source is not in a random pattern but a gradual pattern. We get this conclusion because this is the general rule of the state change of things in real world.

A weight array *A* is defined to show the importance of each factor of controlled variables. Through the weight array *A*, different metric variable has different effect.

Meanwhile, a drop scale factor *S* is defined to express the dropping level during the feedback process. The range of *S* is from *0* to *1*.

The value of manipulated variables can be adjusted according to the feedback value. The feedback value can be calculated by Eq. (2).

$$\Delta MV = S \bullet A \bullet f(E) \quad (2)$$

here ΔMV indicates the feedback value which is the changing value of manipulated variables. Function *f* denotes the transfer function in feedback control system. We can select appropriate transfer function *f* according to different area and systems, here we choose PID (Proportional, Integral, Derivation) control function, which is very simple and efficient in control system, as transfer function to calculate the feedback value.

The values of the dropping scale factor *S* and the controlled variables weight array *A* are set to an adaptive expression according to the total error *E*. So, the feedback adjusting value *ΔMV* is changed following the difference value *E*. According to the value, the system can auto adjust the incoming data rate *R* adaptively. If the total error *E* becomes smaller, the *R* will get smaller, vice versa too. After the feedback adjusting, the whole system will get stable quickly and the system will become load balancing rapidly.

The basic system diagram is shown in Fig. 2. In this system, a monitor measures the value of *CV* periodically. And then the total error *E* is calculated. Then the adjusting feedback value *ΔMV* is generated by multiply the weight array A and the scale dropping factor *S* with the result of *f(E)*. By negative feedback control, the controller will actuate the load shedder to drop incoming data tuples and make the incoming data rate down. After that, the system will become stable rapidly.

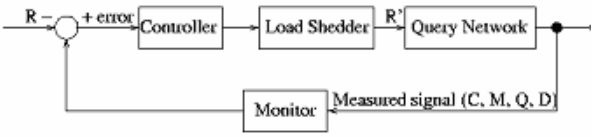


Fig.2. Feedback load-shedding system in DSMS

4. CONCLUSIONS

Previous work on this area mainly takes only one metric factor into account, such as CPU, memory utilization etc.. But it does not satisfy the reality in which several coupled factors should be concentrated. In this paper, an adaptive control-based feedback load-shedding in load management of distributed data stream processing system is proposed. We take four coupled factor, CPU usage ratio, memory utilization, average length of waiting data queue and data tuple delay, into account to implement the control-based feedback load-shedding strategy. Future work should be focused on the selectivity of the feedback parameters to get more efficient and effective, and to decrease the loss of accuracy of queries.

REFERENCES

[1] Aurora Site. http://www.cs.brown.edu/research/aurora/
[2] Medusa. http://nms.csail.mit.edu/projects/medusa/
[3] STREAM Website. http://www-db.stanford.edu/stream/
[4] TelegraphCQ Project. http://telegraph.cs.berkeley.edu/
[5] Borealis. http://www.cs.brown.edu/research/db/borealis/
[6] Argus website. http://www.db.pku.edu.cn/argus/
[7] M. Cherniack, H. Balakrishnan, M. Balazinska, D. Carney, U. Cetintemel, Y. Xing, S. Zdonik. “Scalable Distributed Stream Processing [C]”. In *proceedings of the First Biennial Conference on Innovative Database Systems (CIDR'03), Asilomar*, CA, January 2003: 257-268.
[8] Abhinandan Das, Johannes Gehrke, Mirek Riedewald. “Approximate Join Processing Over Data Streams [C]”. In *Proc. of the 2003 ACM SIGMOD Intl. Conf. on Management of Data*. 2003: 40-51.
[9] Brian Babcock, Mayur Datar, Rajeev Motwani. “Load Shedding for Aggregation Queries over Data Streams [C]”. *Proceedings. 20th International Conference on Data Engineering*, 30 March-2 April 2004: 350-361.
[10] F. Reiss and J. M. Hellerstein. “Data Triage: An Adaptive Architecture for Load Shedding in TelegraphCQ [C]”. In *Pro ceedings of ICDE*, pages 155-156, April 2005.
[11] Y. Chi, H. Wang, and P. S. Yu. “Load Star: Load Shedding in Data Stream Mining [C]”. In *Procs. of the 31st VLDB Conf.*, pages 1302-1305, August 2005.
[12] Yi-Cheng Tu and Sunil Prabhakar.” Control-Based Load Shedding in Data Stream Management Systems [C]”. In *Procs. of DEXA 2005*, p 746-755, Aug 22-26 2005.
[13] Yi-Cheng Tu, Yuni Xia, and Sunil Prabhakar. “Quality of Service Adaptation in Data Stream Management Systems: A Control-Based Approach [C]”. In *Proceedings of 30th International Conference on Very Large DataBases (VLDB'04)*, Toronto, Canada, August 2004.
[14] Hu, Zijing, Li, Hongyan, Qiu, Baojun, et al. “Using control theory to guide load shedding in medical data stream management system [C]”. Source: Lecture Notes in *Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), v 3818 LNCS, Advances in Computer Science - ASIAN 2005: *10th Asian Computing Science Conference*, Proceedings, 2005, p 236-248, Dec 7-9 2005.

Lin Ouyang male, is a Ph.D candidate in School of Information Engineering, Wuhan University of Technology. His research interests are in distributed and parallel processing, Artificial Intelligence and computer network.

Qingping Guo is a Full Professor and a head of Parallel Processing Lab, dean of Computer Technology Institute in School of Computer Science and Technology, Wuhan University of Technology. He graduated from Wuhan University in 1968; from Huazhong University of Science and Technology in 1981 with specialty of wireless technology. He is a holder of K. C. Wong Award of UK Royal Society (1994); was a visiting scholar of City University and of West Minster (1986~1988), Visiting Professor of the UK Royal Society (1994), Visiting Professor of Queen Mary and Westfield College, London University (1997~2000), Visiting Professor of National University of Singapore (2000), Visiting Professor of University Greenwich (2003). He is one of the DCABES international conference founder, was the chairman of DCABES 2001, co-chair of DCABES 2002, the chairman of DCABES 2004 and will be the chairman of DCABES 2007.He has published two books, over 80 Journal papers, edited two DCABES Proceedings. His research interests are in distributed parallel processing, grid computing, network security and e-commence.

The Tasks Allocating in Distributed System by Particle Swarm Optimization

Xiaogen Wang, Wenbo Xu
Education School, Southern Yangtze University
School of Information Technology, Southern Yangtze University
Wuxi, Jiangsu 214122, China
Email: vctwang@sytu.edu.cn

ABSTRACT

Application modules allocation in a distributed computing system, known as tasks allocation problem, is a complex and NP hard problem. The minimization of system costs and the maximization of system reliability are the two important objectives in tasks allocation problem. By combining them efficiently, these two objective optimization problems can be transferred into one objective optimization problem. Different particle swarm optimization algorithms are introduced to solve the optimization problem. Evaluate simulation shows that particle swarm optimization algorithm can solve the tasks allocation problem effectively. The quantum behavior particle swarm optimization algorithm is better than standard particle swarm optimization algorithm.

Keywords: Task Allocation, Particle Swarm Optimization, System Cost.

1. INTRODUCTION

In distributed computing systems such as grid system, an application is divided into a set of modules and allocated to the computers for running in parallel. It is known as tasks allocation problem. There are some running constraints between the tasks, such as running order. The modules will communicate and exchange data each other in running. The minimization of the processing costs and communication costs become the two important goal of the task allocation problem [1]. Meanwhile, the improvement of reliability in distributed computing system is also the key to a good allocation of tasks[2]. Because task allocation problem has been proved NP-hard problem[3], how to allocate the tasks optimally to the computers has attracted more and more researchers. In this paper, we use particle swarm optimization algorithm (PSO) to solve the task allocation problem. And evaluate the performance of standard particle swarm optimization algorithm (SPSO), and quantum behavior particle swarm optimization algorithm (QPSO) by simulate experiments.

2. TASK ALLOCATION IN DISTRIBUTE COMPUTING SYSTEM

As the different number and the heterogeneous structure of computers in a loose coupling distributed computing system, it is need to take the network connection and communication costs into account when allocating the tasks to computers. The optimization of total tasks running time and communication cost between modules become the key to the task allocation problem. Meanwhile, the less running time and communication cost, the higher reliability system will be.

2.1 Network Topology in Distributed Computing System

In a loose coupling distributed computing system, the different network connection of heterogeneous computers will result different communication links and costs when tasks running. Fig-1 shows three typical network topology graphs with 7 computers in a distributed computing system. Where P={pi} i=1,2,⋯,n, p_i is the ith computer in system, n is the size of system. L={l_{ij}} 1<=i<j<=n, is the communication link between computer i and computer j.

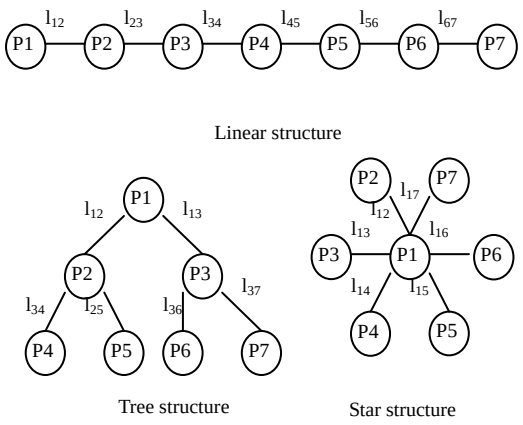


Fig.1. Three Typical Network Topology Graphs

In this paper, we focus on the task allocation problem with ladder and tree connection topology.

2.2 System Costs and Reliability

In task allocation problem, the system costs include the module running costs in different computers, and the communication costs between the modules when running. The running costs and communication costs of the modules are time dependent, thus the more processing and communication time, the more processing costs will it take.

Assume an application consist of r tasks. There are n computers in the distributed computing system. Thus the task allocation problem can be described as:

$X=\{x_{ik}\}$, $1<=i<=r$, $1<=k<=n$

Where $x_{ik}=1$ means the ith module is allocated to the kth computer. If the running time in p_k is e_{ik}, then the total running time of the task is:

$$\sum_{k=1}^{n}\sum_{i=1}^{r} x_{ik}\, e_{ik} \qquad \text{Eq. (2.1)}$$

In the same way, the total communication costs can be described as:

$$\sum_{k=1}^{n-1}\sum_{b>k}\sum_{i=1}^{r}\sum_{i\neq j} u_{kb}\, x_{ik}\, x_{jb}\, (c_{ij} / w_{kb}) \qquad \text{Eq. (2.2)}$$

Where u_{kb} and w_{kb} are the transmission cost and speed of the communication link l_{kb} between module k and module b, is the communication load between module I and module j.

The running costs and communication costs are the total costs of distributed computing system:

$$C(X)=\sum_{k=1}^{n}\sum_{i=1}^{r}x_{ik}e_{ik}+\sum_{k=1}^{n-1}\sum_{b>k}\sum_{i=1}^{r}\sum_{i\neq j}u_{kb}x_{ik}x_{jb}(c_{ij}/w_{kb}) \quad \text{Eq. (2.3)}$$

As to the system reliability, it can be represented as the probability of the success running of the task. It depends on the allocation of modules in system. In general, the reliability of computer k follows the Poisson Distribution $e^{-\lambda_k\sum_{i=1}^{r}x_{ik}e_{ik}}$. The reliability of communication link l_{kb} follows the Poisson distribution $e^{-\mu_{kb}\sum_{i=1}^{r}\sum_{i\neq j}x_{ik}x_{jb}(c_{ij}/w_{kb})}$ too. So the reliability of the distributed computing system is:

$$R(X)=\prod_{k=1}^{n}e^{-\lambda_k\sum_{i=1}^{r}x_{ik}e_{ik}}\prod_{k=1}^{n-1}\prod_{b>k}e^{-\mu_{kb}\sum_{i=1}^{r}\sum_{i\neq j}x_{ik}x_{jb}(c_{ij}/w_{kb})} \quad \text{Eq. (2.4)}$$

2.3. Optimization Objective

In the task allocation problem of distributed computing system, there are two parts of the optimization, first is the minimization of running costs, then the maximization of the system reliability. In order to combine them into one optimization objective, we introduce parameter α to converse the maximization of reliability to the minimization. So the optimization objective can be described as:

$$MinZ \quad (x)=C(X)+\alpha/R(X) \quad \text{Eq. (2.5)}$$

$$\text{s.t.} \quad \sum_{k=1}^{n}x_{ik}=1 \qquad \forall i=1,2,...,r \quad \text{Eq. (2.6)}$$

$$\sum_{i=1}^{r}m_i x_{ik}\le M_k \qquad \forall k=1,2,...,n \quad \text{Eq. (2.7)}$$

$$\sum_{i=1}^{r}s_i x_{ik}\le S_k \qquad \forall k=1,2,...,n \quad \text{Eq. (2.8)}$$

$$x_{ik}\in\{0,1\} \qquad \forall i,k$$

Where α is used to adjust the weighting of reliability.

3. PARTICLE SWARM OPTIMIZATION ALGORITHM

Particle swarm optimization algorithm (PSO) is inspired by the behavior of bird flocking[4]. It is applied to the field of complex optimization problems and has gotten good optimization performance in many problems. In PSO, every possible solution is imagined as a point in D dimension space, called "particle". Each particle has a fitness value by fitness function. Every particle flies in the searching space with a certain speed, and adjust it's speed and position by experience itself and other particles. There are many kinds of PSO algorithms developed from initial PSO for different optimization problems. In this paper, we use two of them to the task allocation problem and evaluate their allocation performance. They are standard particle swarm optimization algorithm (SPSO) and quantum behavior particle swarm optimization algorithm (QPSO)[5].

3.1 Standard Particle Swarm Optimization Algorithm

In standard particle swarm optimization algorithm, if $f(x)$ is the objective function of minimization, the best solution of particle i at time t can generate by iteration:

$$p_i(t)=\begin{cases}p_i(t) & f(x_i(t+1))\ge f(p_i(t+1))\\ x_i(t+1) & f(x_i(t+1))<f(p_i(t+1))\end{cases} \quad \text{Eq. (3.1)}$$

The best solution of the swarm is:

$$p_g(t)\in\{p_0(t),\ p_1(t),\ \cdots,\ p_m(t)\}\mid f(p_g(t))=\min\{f(p_0(t)),\ f(p_1(t)),\ \cdots,\ f(p_s(t))\} \quad \text{Eq. (3.2)}$$

The evolutionary iteration include the updating of particle's velocity and position as below:

$$v_{id}(t+1)=\chi*(v_{id}(t)+c_1r_{1d}(t)(p_{id}(t)-x_{id}(t))+c_2r_{2d}(t)(p_{gd}(t)-x_{id}(t))) \quad \text{Eq. (3.3)}$$

$$x_{id}(t+1)=x_{id}(t)+v_{id}(t+1) \quad \text{Eq. (3.4)}$$

Where d=1,2,…,D, D is the dimension of search space, i=1,2,…,m, m is the particle swarm size, t is the current swarm generation. c_1 and c_2 are two accelerate factors. r_1 and r_2 are two random numbers in [0,1]. χ is the constriction factor. It can get from c_1, r_1, c_2, and r_2.

3.2 Quantum Behavior Particle Swarm Optimization Algorithm

The standard particle swarm optimization algorithm has the limitation in particle motion tracks and search space. The quantum behavior particle swarm optimization algorithm is proposed to improve the performance of standard particle swarm optimization algorithm. Assume that each individual particle move in the search space with a δ potential on each dimension, of which the center is the point p_{ij}. For simplicity, we consider a particle in one-dimensional space, with point p the center of potential. By solving Schrödinger equation of one-dimensional δ potential well, we can get the probability distribution function D.

$$D(x)=e^{-2|p-x|/L} \quad \text{Eq. (3.5)}$$

Using Monte Carlo method, we obtain

$$x=p\pm\frac{L}{2}\ln(1/u),\quad u\sim U(0,1) \quad \text{Eq. (3.6)}$$

The above is the fundamental iterative equation of quantum particle swarm optimization algorithm.

In [7], a global point called Mainstream Thought or Mean Best Position of the population is introduced into PSO. The global point, denoted as p, is defined as the mean of the personal best positions among all particles. That is

$$p_m(t)=\sum_{i=1}^{N}p_i(t)/N=\left(\sum_{i=1}^{N}p_{i1}(t)/N,\sum_{i=1}^{N}p_{i2}(t)/N,...,\sum_{i=1}^{N}p_{id}(t)/N\right) \quad \text{Eq. (3.7)}$$

Where N is the population size and P_i is the personal best position of particle i. Then the value of L is evaluated by $L=2\beta\cdot|p_j(t)-X_{ij}(t)|$ and the position are updated by

$$p_d(t+1)=\varphi*p_{id}(t)+(1-\varphi)*p_{gd}(t) \quad \text{Eq. (3.8)}$$

$$x_{id}(t+1)=p_d(t+1)\pm\beta*|p_m(t)-x_{id}(t)|*\ln(1/\mu) \quad \text{Eq. (3.9)}$$

where parameter β is called Contraction-Expansion (CE) Coefficient, which can be tuned to control the convergence speed of the algorithms. φ and σ are the randomized number between 0 and 1 in each iteration.

4. TASK ALLOCATE SIMULATION

We introduce SPSO and QPSO to allocate the application modules to the different computers. The ladder and tree topological network connection of system are used in the allocate simulation. The simulation platform is a 2.5GHZ PC with 256MB RAM and the Matlab 7. In order to simulate the distributed computing system and make the algorithm working efficiently, we use the following parameters. The parameters c_1 and c_2 are set to 2.05. The population size is set to 80. c_{ij} and e_{ij} are set randomly to 15-25. λ and μ are set randomly to 0.00005-0.0001. m_i and s_i are set 1-60, M_i and S_i are set randomly to 100-200, etc. Each optimization algorithm is run 20 times. Table1 and table2 show the results of simulation experiments.

Table 1. Simulation Experiment Results with Tree Topological Connection

System Size		SPSO			QPSO		
n	r	Max	Min	Average	Max	Min	Average
7	9	93.6722	74.3650	85.5695	89.0307	40.6558	71.7366
7	13	166.2508	131.5044	148.2068	137.7962	110.0627	128.3208
9	11	128.0658	118.7754	125.1382	131.7047	113.2109	120.9699
9	17	237.3991	208.1841	226.3124	234.1805	195.6252	212.9360

Table 2. Simulation Experiment Results with Ladder Topological Connection

System Size		SPSO			QPSO		
n	r	Max	Min	Average	Max	Min	Average
7	9	95.8805	81.3541	89.0391	83.4153	63.8079	71.9755
7	13	157.2537	120.3365	145.6875	145.1085	116.5305	131.6023
9	11	135.4277	120.3415	129.3551	127.9360	106.3353	117.0684
9	17	240.5342	214.3810	226.5536	228.5772	187.0080	217.6183

From table and table2, we can see that both standard particle swarm optimization algorithm (SPSO) and quantum behavior particle swarm optimization algorithm (QPSO) can allocate the modules to the computers efficiently with reasonable costs. Comparing QPSO to SPSO, the QPSO can get better performance on task allocate problem than SPSO in different system configurations. The QPSO algorithms can reach better allocation of application modules in tasks allocation problem.

5. CONCLUSIONS

The task allocation problem in distributed computing system is a complex and hard problem. In order to allocate the application modules to computers efficiently, one should take not only the system running costs, but also the system reliability into account. Particle swarm optimization algorithm as a heuristic method can used to solve the tasks allocation problem effectively. QPSO as an improvement of standard particle swarm optimization algorithm, it can obtain better allocate results when used to the tasks allocation problem.

REFERENCES

[1] C.H. Lee, K.G. Shin, Optimal task assignment in homogeneous networks, IEEE Transactions on Parallel and Distributed Systems 8(1997) 119–129.

[2] S. Kartik, S.R. Murthy, Task allocation algorithms for maximizing reliability of distributed computing systems, IEEE Transactions on Computers 46 (1997) 719–724.

[3] V.M. Lo, Task assignment in distributed systems, Ph.D. dissertation, Department of Computer Science, University of Illinois, October, 1983.

[4] Eberhart R.C, Kennedy J. A New Optimizer Using Particle Swarm Theory. 6th International Symposium on Micro Machine and Human Science, Piscataway, NJ, Nagoya, Japan, 1995, 39-43.

[5] Sun J, Feng B and Xu WB. Particle Swarm Optimization with Particles Having Quantum Behavior. IEEE Congress on Evolutionary Computation, 2004, 325-331

[6] Clerc M, Kennedy J. The Particle Swarm-Explosion, Stability, and Convergence in a Multidimensional Complex Space. IEEE Transaction on Evolutionary Computation, 6(1): 58-73, 2002.

[7] Sun, J., Xu, W.-B., Feng, B. A Global Search Strategy of Quantum-behaved Particle Swarm Optimization. Proc. 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore (2004) 111-115

Xiaogen Wang is a Associate Professor in Information and Education Technology Department, School of Education, Southern Yangtze University. He graduated from Zhejiang University in 1987 with specialty of Physics. He was a research member of the machine tool's numerical control system project between 1987 and 1992; then was a software engineer in Wuxi MEB Software Engineering Co. ltd., and last become a teacher of Southern Yangtze University. His research interest includes multimedia technology, intelligent computing, etc.

A New Task Scheduling Algorithm Using Dynamic Prediction Adjustment and Task Flow Shaping for Grid Computing*

Shenwei Tian, Turgun, Long Yu, Jiong Yu
College of Information Science and Engineering, Center of Networking
Xinjiang Universtiy, Xinjiang Shengli Road, Urumchi, Post code 830046 China
Email: tsw@xju.edu.cn

ABSTRACT

According to the autonomy, heterogeneity, and distributed nature of grid computing system, we propose a new grid scheduling algorithm based to reduce average task response time with dynamic prediction adjustment and task flow shaping. The algorithm uses history data and the recent task request time, task completion time, and network communication delay, to predict the future task response time at each computing node. Based on the prediction result, tasks will be assigned to computing nodes which are predicted to have less work load and better performance in the near future. The resource utilization can be improved with both the dynamic adaptation algorithm and the task flow shaping algorithm. Experimental results show that our approach outperforms existing scheduling algorithms (e.g. random scheduling) in terms of task response time and throughput.

Keywords: Prediction, Response Time, Task Flow Reconstruction, Load Balance

1. INTRODUCTION

Task Scheduling is an important issue in the area of grid computing. Task scheduling algorithms are used in large-scale computing grid and assign each task to the node with the shortest expected completion time. The main metric in scheduling decision is the task completion time. Currently, there are several existing static scheduling algorithms such are Min-min, Max-min, GA, Sufferage and XSuffrage, etc. Also, several dynamic scheduling algorithms such as MET(minimum execution time), MCT(minimum completion time), SA(switching algorithm), KPB(K-percent best), OLB (opportunistic load balancing) are available. Due to the dynamic nature of grid resources, static scheduling algorithms cannot efficiently utilize grid resources. In comparison, dynamic algorithms perform well in various environments and can effectively adapt to dynamic grid environment.

However, existing dynamic scheduling algorithms usually require the control of each grid node, which is impractical in grid environment with autonomous grid nodes. In addition, some other dynamic scheduling algorithms have too strong assumptions in the extent of dynamics of grid nodes. For example, some algorithms do not consider the communication overhead of each node, and cannot be applied to real grid environments. Some algorithms perform real-time load monitoring on each node, and incur huge communication overhead. Furthermore, considering the latency and it variation in wide area networks (e.g., Internet), it is extremely difficult to measure the real-time load information of each node. Some other traditional scheduling algorithms apply the policy that assigns tasks to grid nodes'task queue according to current prediction results. However, this approach handles bursty tasks poorly since the length of task queue can be suddenly increased. As a result, when the workload after the assignment varies significantly, there will be a considerable error regarding predicted task completion time.

As a result, we study a task scheduling algorithm that performs dynamic prediction adaptation of task response time and task flow shaping. The proposed algorithm is capable of adapting to dynamic grid computing environment. It dynamically predicts the task completion time on computing nodes according to the history performance information. Then it assigns each task to the node that is expected to have the least response time. Also, the algorithm shapes the task flow so that the queue length of each computing node can be controlled. Consequently, it effectively decreases the prediction error due to too long queuing delay and avoids the resource waste due to underutilization of each node. Through experiments, it is shown that our algorithm can achieve accurate prediction and high resource utilization in grid computing environments.

2. BACKGROUND OF SCHEDULING IN GRID COMPUTING

In grid computing systems, a computing node consists of heterogeneous sub-nodes, which can be denoted by C=(c1, c2,⋯,cn). Let's denote all tasks to T=(t1,t2,⋯,tm). Tasks are randomly delivered to the scheduler module and each task is assigned by the scheduler to a computing node. Different computing nodes have different performance, as a result, the execution time of the same task on different nodes can be quite different. On the other hand, each computing node has a waiting queue L, which can be used to measure the utilization of the node. The scheduling algorithm is designed to determine how to assign tasks according to current resource utilization such that the total execution time of tasks is minimized. Let's assume waits(ti) is the queuing delay of task ti, commu(ti,cj) is the communication delay of task ti assigned to node cj, waitl(ti,cj) is the queuing delay of task ti after it is assigned to node cj, exe (ti,cj) is the execution time of task ti on node cj. Then the response time of task ti can be calculated as:

$$tfinish(ti,cj)= waits(ti) +commu(ti,cj) + waitl(ti,cj) +exe (ti,cj). \quad (1)$$

The scheduler should select the node that incurs the least expected tfinish(ti,cj).

3. THE RESPONSE TIME-BASED PREDICTION ALGORITHM

The model of task scheduling in grid systems is depicted in Fig.1. Task request is assigned to the scheduler. After the scheduler receives the request, it applies a certain scheduling policy/algorithm to assign the task to a computing node. The computing node will send the result back to the scheduler after

* Supported by the National Natural Science Foundation of China under Grant No. 60563002.

finishing the task. According to the time when the task is assigned to the node and the time when the node sends the result to the scheduler, we can determine the response time of the task. This paper proposes a scheduling algorithm that uses the history response times to predict future response time.

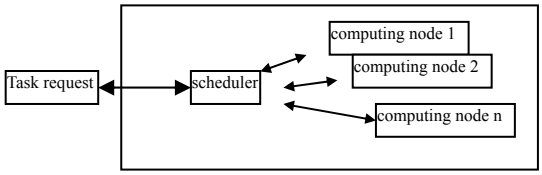


Fig.1. Model of task scheduling

3.1 prediction model

With the principle of locality, a computing node's current performance is close to its recent performance history. To predict the response time on the computing node, we can exploit its recent response times. Suppose CF=(s1,s2,…,sp) is the vector of the recent response times on the computing node, where p is the number of history response times. We can use the previous p response time to predict the p+1th response time on the node. We have:

$$s_{p+1} = \frac{1}{p} * \sum_{i=1}^{p} s_i + \varepsilon \qquad (2)$$

where ε is the adjustment parameter. Equation (2) uses the average of p most recent task response times to predict future task response time. In order to cancel some noises, we use adjustment parameter ε. The value of ε has impact on the prediction accuracy. Without carefully adjusting the value of ε, we may have large prediction error. Therefore, this paper gives an adaptive algorithm to adjust the value of ε according to the variation of history response time.

Definition 1: Response time waving rate (RWR): given a sequence CF=(s1,s2…st),， if sj-1<sj and sj>sj+1, or sj-1>sj and sj<sj+1 （1<j<t）, then work load waves at j and j is the waving point. The RWR=the number of waves/t/. RWR reflects the frequency of changes of task response time.

Definition 2: If ε=0, then we call it zero adaptation. It means that there is no adjustment for prediction.

Definition 3: Given task response time sequence CF=(s1,s2…sp), if $\varepsilon = \sqrt{\frac{\sum_{i=1}^{p}(s_i-\mu)^2}{p}}$, （$\mu = \frac{1}{p}\sum_{i=1}^{p} S_i$）, then it is the unsigned standard deviation adjustment.

Definition 4: Given task response time sequence CF=(s1,s2…sp), if $S_p >= S_{p-1}$, then $\varepsilon = \sqrt{\frac{\sum_{i=1}^{p}(s_i-\mu)^2}{p}}$, if $S_p < S_{p-1}$ then $\varepsilon = -\sqrt{\frac{\sum_{i=1}^{p}(s_i-\mu)^2}{p}}$. This is the signed standard deviation adjustment.

3.2 Evaluation and Analysis of the Prediction Algorithm

We conduct experiments on the task response time prediction. We evaluate 200 predictions of task response time on a non-dedicated computing node, p is chosen to be 20. The results are shown in Fig.2 and 3. Fig.2 shows the prediction results when RWR is high and we can see that the zero adjustment has smaller prediction error than the signed standard deviation adjustment. Fig.3 shows the prediction results when RWR is low and we can see that the signed standard deviation adjustment has smaller prediction error than the zero adjustment.

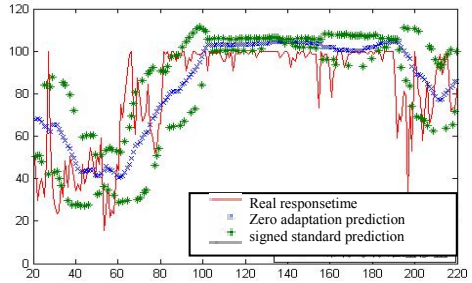


Fig.2. Comparison of prediction based high RWR

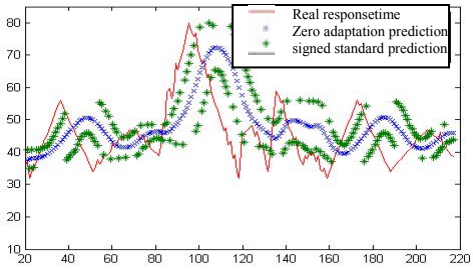


Fig.3. Comparison of prediction based low RWR

We perform experiments using 4 heterogeneous computers, and they have Intel Celeron 933MHz CPU+ 128M memory, Intel Pentium CPU 1.6GHz+256M memory, Intel Pentium 2.4GHz+512M memory, and Intel Celeron 3.06GHz+512M memory, respectively. We evaluate the average prediction errors for the response time of 1000 randomly generated tasks on these computers with different work loads.

The experimental results are shown in Tables 1 and 2. As can be seen, the unsigned standard deviation adjustment produces

Table 1. RWR=65.%

Adjustment algorithm	prediction error
zero adjustment	0.2656
unsigned adjustment	0.3527
signed adjustment	0.3042

Table 2. RWR=8.22.%

Adjustment algorithm	prediction error
zero adjustment	0.1856
unsigned adjustment	0.2529
signed adjustment	0.1698

the largest prediction errors among the three adjustment methods regardless of the value of RWR. When RWR is high, the zero adjustment has the least prediction error. When RWR is low, the signed standard deviation adjustment has the least prediction error. Therefore, we can conclude that, in order to reduce prediction error, we should use the zero adjustment when RWR is high and use the signed adjustment when RWR is low.

4. THE PROPOSED SCHEDULING ALGORITHM

4.1 The Algorithm of Dynamic Prediction Adjustment

Algorithm 1: given node ck and p history task response times (s1,s2…sp), we can predict the next task response time trsk following:

1、 compute the node c_k's RWR, which is denoted by RWRk;

2、 if RWRk > α , ε =0 where α is the threshold

else if $s_p < s_{p-1}$ $\varepsilon = -\sqrt{\frac{\sum_{i=1}^{p}(s_i-\mu)^2}{p}}$

else $\varepsilon = \sqrt{\frac{\sum_{i=1}^{p}(s_i-\mu)^2}{p}}$

3、 $s_{p+1} = \frac{1}{p} * \sum_{i=1}^{p} s_i + \varepsilon$;

4、 $trs_k = s_{p+1}$

4.2 The Algorithm for Task Shaping

The basic idea is as follows: arriving tasks are initially put into the waiting queue of the scheduler. The scheduler selects the computing node that is the best one in the resource set and assigns the task to that computing node. If the computing node cannot return result within the time threshold, then the computing node will be deleted from the resource set and the scheduler will not consider it as candidate computing nodes until the computing node returns the pending result. This approach guarantees that the queue length of each computing node can be limited. Also, the algorithm only predicts the performance of nodes in the resource set so that the computational complexity of prediction can be decreased. The algorithm is as follows:

Initialize resource set , RS, which has n computing nodes. For each node in RS, select a pre-defined time threshold TL_k(1<=k<=n), which is initialize to be ∞. The timer TCk=0 (1<=k<=n) for each node.

Algorithm 2: Synchronized threads for managing the resource set:

If computing node c_k （1<=k<=n）finishes a task and returns the result to the scheduler, and if the computing node is not in the resource set, then include the node in the resource set and re-compute the expected task response time on the node, denoted by trsk . Let $commu_k$ the communication delay between ck and the scheduler.

Compute the current elapse time $WAIT_k$(1<=k<=n) since a task has been assigned to node ck,. If $WAIT_k > TL_k$, the remove the node ck from the resource set until the node returns result to the scheduler.

Algorithm 3: Scheduling Algorithm

1. For the task t_i in the waiting queue of the scheduler, calculate the t_i's queuing delay at the scheduler $schwait_i$;
2. If RS is empty, wait until RS becomes non-empty. For every computing node c_k in RS,
   if (TC_k>0)
   if (trs_k - TC_k <= s_{p+1}) trs_k = s_{p+1} // s_{p+1} is the predicted task response time calculated with Algorithm 1
   else trs_k = trs_k – TC_k
3. Reset timer TC_k and start the timer;
4. c_j=getMin(trs_k) (1<=k,j<=n);
5. Assign task ti to computing node c_j; reset and start the timer TC_j; update the node c_j's expected task response time trs_j as:
   trs_j =trs_j+ s_{p+1} -schwaiti-2*$commu_j$; // $commu_j$ is the latest communication delay between node c_j and the scheduler
6. Go to step 1.

4.3 Experiment Results and Analysis

With the 4 computers used in the previous experiments, we measure the average task execution delay (in msec) when each computing node is lightly loaded. The delays on these nodes are 1252、1506、1923、2058, respectively. The communication delays (in msec) are 252,50,45,2, respectively. We let each computing node non-dedicated (i.e., there is some background tasks on the node) and set the number of history task response times p to be 20. The threshold used for updating RWR is 0.3. In the experiment, there are 600 tasks randomly delivered to the scheduler. We evaluate the performance of scheduling with different scheduling algorithms. To achieve high confidence of evaluation, each experimental case is repeated 10 times.

From Table 3, the random scheduling algorithm causes unbalanced work load on the computing nodes and brings significant delay. The reason is that the algorithm does not consider heterogeneity of computing nodes. The zero adjustment performs better than the unsigned standard deviation adjustment. The signed standard deviation adjustment is the second best approach. Our dynamic prediction adjustment and task flow shaping scheduling algorithm can adapt the scheduling decision to the dynamic system, and assign tasks adaptively. Therefore, its average task response time is the least. Compared to the random scheduling, the delay of our approach is decreased by 30.7%.

Table 3. Performance comparison of five scheduling approaches

Adjustment algorithm	Finished tasks of computing node 1	Finished tasks of computing node 2	Finished tasks of computing node 3	Finished tasks of computing node 4	General response time
random scheduling	155	149	150	146	365963
zero adjustment	135	186	152	127	270034
unsigned adjustment	132	190	158	120	293576
signed adjustment	130	183	161	126	275167
Proposed Scheduling Algorithm	135	185	155	125	253598

5. CONCLUSIONS

This paper studies a new task scheduling algorithm that uses dynamic prediction adjustment and task flow shaping to address the weakness of existing scheduling algorithm in grid computing systems. The algorithm improves the prediction accuracy with dynamic prediction adjustment and effectively reduces the prediction error due to overlong queuing delays through task flow shaping. When there are bursty tasks, the algorithm significantly outperforms other scheduling algorithms. Through experiments, we prove that the proposed scheduling algorithm is a successful solution for task scheduling in grid computing systems. In the future, we will

refine the algorithm and apply it to the digital library system at Xinjiang University.

REFERENCES

[1] BRAUN T D,SIEGEL H J,BECK N, et al,"A comparisonstudy of static mapping heuristics for a class of metatasks on heterogeneous computing systems"[A]. *8th IEEE Heterogeneous Computing Work-shop* (HCW`99)[C],1999.

[2] MAHESWARAN M,ALI S,SIEGEL H J,et al,"A omparison of Dynamic Strategies for Mapping a Class of Independent Tasks onto Heterogeneous Computing Systems,"Technical Report, School of Electrical and Computer Engineering, Purdue University,1999.

[3] Wei TY,Zeng WH, Huang BB,"Scheduling algorithm based on modified Min-Min in grid,"*Computer Applications,* 2005,25(5),pp.1190−1192 (in Chinese with English abstract).

[4] Maheswaran M,Ali S,Siegel HJ, Hensgen D,Freund RF, "Dynamic matching and scheduling of a class of independent tasks onto heterogeneous computing systems," in *Proc. of the 8th Heterogeneous Computing Workshop* (HCW'99),Washington: IEEE Computer Society Press, 1999,pp.30−44.

Shengwei Tian (1973-) , male, Ph.D candidate. Born in Si Chuan. Lecture of Xinjiang University. Research area: Computer networks and intelligent techniques

Turgun(1958-),male, Professof of Xinjiang University. Research Area: Intelligent techniques

Long Yu (1974-), female, M.S. Associate professor of Xinjiang University. Research area: computer network and its applications.

Jiong Yu (1964-) ,male, Professof of Xinjiang University. Research Area: Computer networks

Optimizing the Result of Capturing Concurrency within an Activity *

Qizhao Lin [1], Tong Li [2]
[1] School of Information Science and Engineering, Yunnan University
[2] School of Software, Yunnan University
Kunming, 650091, China
Email: [1] senly2004@126.com, [2] li@ynu.edu.cn

ABSTRACT

Capturing the software process concurrency as far as possible, this can enhance the software production efficiency and the software quality. In fact, it can not away to shorten the software run time while considering the activity run time as a main factor. Supposes every activity run time is knowable, this paper gives an algorithm to optimize the result of capturing concurrency within an activity, which is base on the record of activity concurrency relation and some special attribute.

Keywords: Software Evolution, Algorithm Optimization, Capturing Concurrency

1. INTRODUCTION

To enhance the software production efficiency and the software quality, it is a persistence research for the software engineering researchers who have done much work for it and have given many efficiency methods. Capturing the software process concurrency as far as possible is a way of shortening the time of software development.

In a software process, there are many activities can be executed concurrency. It can capture concurrency within an activity. The author of the conference [3] has given many methods to mining for concurrence in software process for evolution which includes a method to capturing concurrency within an activity.

As considering every activity run time, some software process can not shorten its run time although it executed concurrency enough. The following content will discover the instance show the activity run time can not always be shorten while its has refined into many concurrent activities, then give an algorithm to optimize the result of capturing concurrency within an activity.

2. CAPTURING CONCURRENCY WITHIN AN ACTIVITY

To capture concurrency within an activity, it uses Refining_Activity [3] algorithm to refining an activity into a concurrent activity set.

According to Algorithm Refining_Activity, the activity *a* enclosed in doted lines in Fig.1(a) is refined to a process segment enclosed in doted lines in Fig. 1(b) in which activities a_1, a_2 can be executed concurrently.

Suppose activity *a* should take t_0 to executed completely. After captured the activity *a*, activity a_1's run time is t_1 and a_2's run time is t_2. $t1 < t_2 < t_0$. If a_1 and a_2 started at the same time, activity *a* takes t_2 to be executed completely. Because $t_2 < t_0$, the activity *a*'s run time is shorten after capture. The above work is called the first times captured.

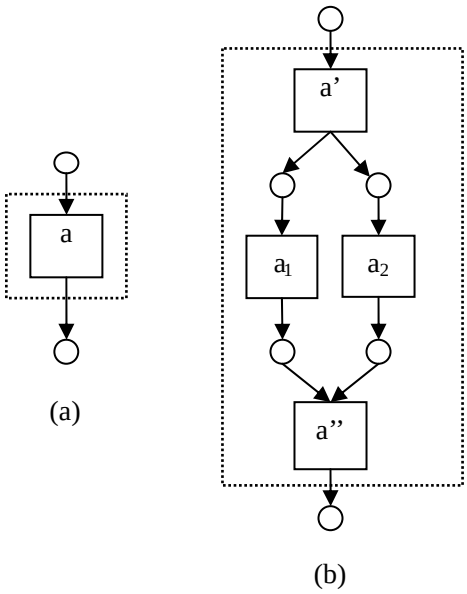


Fig.1. Refining an Activity into Concurrent Activities

Suppose activity a_1 can refined into activity a_{11} and activity a_{12} and activity can not be refined. Now, a_{11}, a_{12} and a_2 are concurrent activities. Activity a_{11}'s run time is t11 and activity a_{12}'s run time is t_{12}, and $t_{12} < t_{11} < t_2$. If a11 , a_{12} and a_2 started at the same time, activity a takes t_2 to be executed completely. The above work is called the second times captured.

In this case, the run time of activity *a* is shortened from t_0 to t_2 after the first times captured. But, the second times captured has not shorten the activity *a*'s run time.

Through the previous example, it can draw the conclusion that the activity's run time can not always be shortened by its enhanced concurrency. The part of the result of capturing concurrency within an activity, which can not shorten the global, is should be optimized in this paper.

3. PICK UP SPECIAL INFORMATION

The Refining_Activity algorithm can not give too much information, such as run time of activity, so it need to pick up special information when capturing concurrency within an activity. The special information include the run time of every activity and the one-many relationship which show an activity can be refined to many concurrent activities. The run time of every activity includes the activity's original run time and the shortest run time of its refined concurrent activities.

Definition 3.1: original run time. If an activity has not been

* The project is supported by National Natural Science Foundation of China under Grant NO.60463002.

refined and takes some time to be executed. Such time is the activity's original run time.

Definition 3.2: updated run time. If an activity has been captured currency as far as possible and takes some time to be executed completely. Such time is called the activity's updated run time.

Definition 3.3: sequence activities. If many activities should be executed in sequence, such activities are called sequence activities.

ADT

```
// TElemType
  typedef struct{
        float oldcost;          //original run time
        float newcost;          //updated run time
        bool isSequence; //  whether  its  refined  activities  are
sequence activities
}TElemType;

//CSNode
typedef struct CSNode{
              ElemType data;
              struct CSNode * firstchild, * nextsibling;
}CSNode, * CSTree;
```

Definition 3.4: concurrency model and special attributes tree. If an object instanced by the CSNode struct, such object is called concurrency model and special attributes tree.

Compute the Run time after Refined

For optimizing the result of capturing concurrency within an activity, it must compute every activity's updated run time. So the following algorithm uses Depth_Fisrt Search strategy to compute concurrency model and special attributes tree nodes' data.

Algorithm 1: Compute updated run time.
Input: The concurrency model and special attributes tree.
Output: The concurrency model and special attributes tree which has update its updated run time.

```
void ComputeNewCost(CSTree &CST){
        CSNode * Child = CST->firstchild;
        if(!Child){
                CST->data.newcost = CST->data.oldcost;
        }
        else{
                 while(Child) {
                       ComputeNewCost(Child);
                       Child = Child->nextsibling;

                 }
                 float newMaxCost = GetMaxNewCost(CST);
                CST->data.newcost = newMaxCost;
            }
}
```

Algorithm 2: Get the max *newcost* from the data of a CSNode node's child nodes
Input: A CSTree node
Output: The max newcost value

```
float GetMaxNewCost(CSTree &CST){
        float newMaxCost = 0;
        CSNode * Child = CST->firstchild;
        if(CST->data.isSeriate)        {
              while(Child){
               newMaxCost += Child->data.newcost;
               Child = Child->nextsibling;
              }
           }
           else {
              while(Child) {
                if(newMaxCost < Child->data.newcost) {
                     newMaxCost = Child->data.newcost;
                }
                Child = Child->nextsibling;
              }
          }
          return newMaxCost;
}
```

If the CSTree node's child nodes are running in Sequence, the max *newcost* is the sum of its child nodes' *newcost*.

Optimization Algorithm

The aim of optimization is to find each part of an activity captured result, which can not influence in the activity's global efficiency, then cut it. The following algorithm uses Breadth_Fisrt Search strategy.

Algorithm 3: Optimize the Result
Input: The root of a concurrency model and special attributes tree.
Output: An Optimized concurrency model and special attributes tree.

```
void Optimize(CSTree &CST){
              ComputeNewCost(CST);
        float newMaxCost = GetMaxNewCost(CST);
        CSNode * Child = CST->firstchild;
        while(Child){
                    if(newMaxCost >= Child->data.oldcost){
                    Child->firstchild = NULL;
                    Child->data.newcost = Child->data.oldcost;
                    }
               Child = Child->nextsibling;
              }
}
```

4. EXAMPLE

Suppose activity a_0 can use the concurrency model and special attributes tree which show as Fig 2 to capture its concurrency. Each node's first number is its *oldcost* and the second number is its *newcost* value. Each node's *oldcost* is equal to its *newcost* when concurrency model and special attributes tree is initializing. a_x is activity's serial number. The false or true is value of node's *isSequence*.

The Fig 3 shows the tree which has used the algorithm 1 to update its updated run time. Obviously, a_0' has been mined into a_{111}, a_{112}, a_{121}, a_{122}, a_{21}, a_{22}, a_{23}, a_{32} and a_{32} which include tow sequence activities.

According to the algorithm 3, a_2's child nodes have been cut and recover a_2's *newcost* to 15, because a_1's *newcost* is 32 and its a_1's *newcost* is the biggest of a_0's child nodes'*newcost*, and 32 is bigger than the a_2's *newcost*. Also a_{11}'s child nodes have been cut and recover a_{11}'s *newcost* to 15, because a_{12}'s *newcost* is 32 and a_{12}'s *newcost* is the biggest of a_1's child nodes'*newcost*, and 32 is beigger than the a_{11}'s *newcost*.

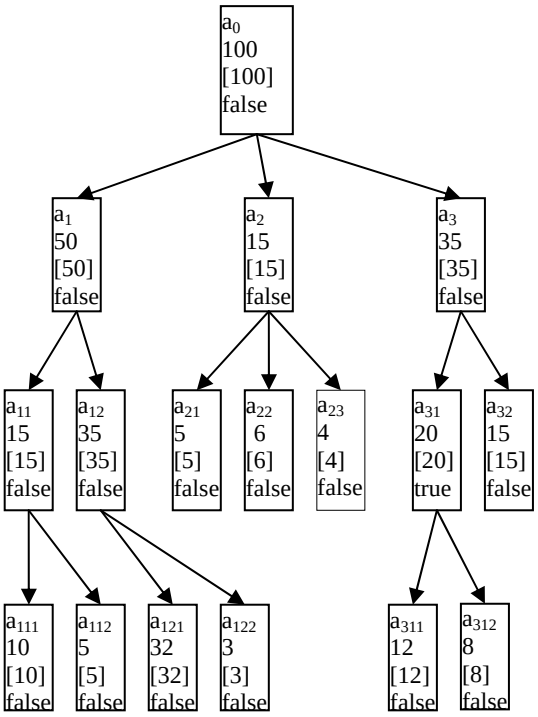


Fig.2. Activity a_0's initialization concurrency model and special attributes tree

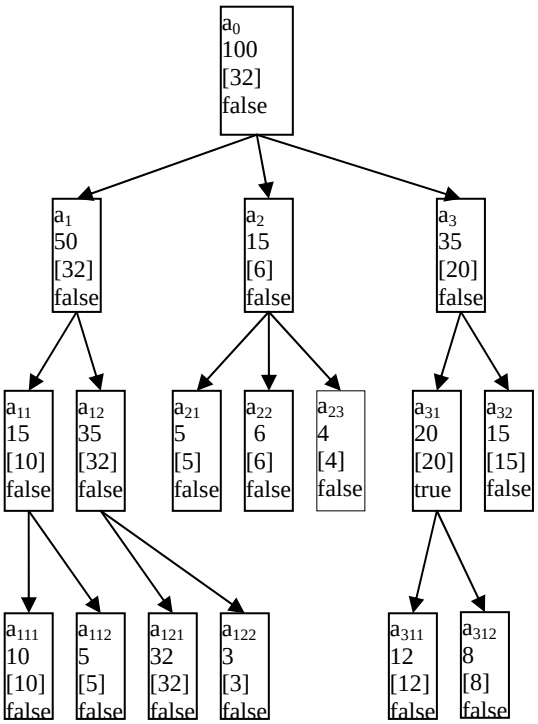


Fig.3. Activity a_0's updated concurrency model and special attributes tree

The Fig4 show the result of the optimizing the activity a_0's updated concurrency model and special attributes tree. Also it is the finally result of capturing concurrency within an activity

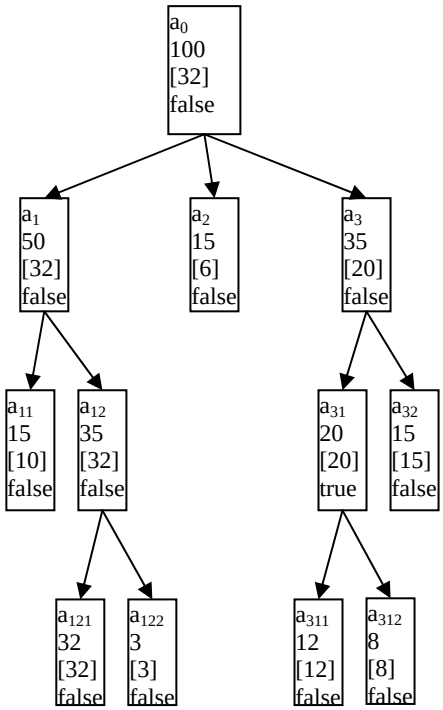


Fig.4. Activity a_0's optimization concurrency model and special attributes tree

Obviously, after optimization, a_0' has been mined into a_{11}, a_{121}, a_{122}, a_2, a_{32} and a_{32} which include tow sequence activities. This result has not influence in the activity a_0's final run time, but it reduce the sum of the a_0's concurrency activities.

5. CONCLUTIONS

Base on the achievement of conference [1] and conference [1], this paper brings out a method to optimize the concurrency part which can not influence in the activity's global efficiency, and its example can work by this method.

REFERENCES

[1] T. Li, H. Yang and J. Jiang, "Mining for Concurrency in Software Process for Evolution", *Proceedings of the 10th Joint International Computer Conference*, International Academic Press, Beijing, 2004, pp.478~483.

[2] Yan Weiming, Wu Weimin, *Data Structure*. Tsinghua University Press, Beijing, 1996, pp.136~137.

[3] Li Tong, Kongbing, Jin Zhao *et al*, *Software Concurrent Development Process* , Science Press, Beijing, 2003, pp.88~98.

Study on Active Queue Management Algorithms*

Ping Hou[1,2], Zhiquan Wang[1]
[1]Department of Automation, Nanjing University of Science & Technology, Nanjing 210094, China
[2]Department of Business Administration, Nanjing College for Population Programme Management
Email: [1]hp_nj@sohu.com

ABSTRACT

In this paper, we mainly study Active Queue Management (AQM) algorithms for Internet congestion control, including RED, ARED, REM, BLUE and so on. Meanwhile, we analyzed their mechanisms, sum up the advantage and disadvantage of algorithms. The research direction of AQM in the future was discussed.

Keywords: Internet Congestion Control, AQM, RED, REM, BLUE

1. INTRODUCTION

Nowadays, the network traffic is increasing exponentially due to the integration of enormous network with many different service providers[1], users and protocols. Internet is suffering more and more performance depravation problems, such as the packet loss rate increases, the end-to-end delay increases, the network throughput decreases, and the network system may go through congestion collapse.

In the modern day Internet, there has been a strong demand for QoS (Quality of Service) and fairness among flows. As a result in addition to the sources, the links are also forced to play an active role in congestion control and avoidance.

In this paper, we introduce and compare some main AQM (Active Queen Management) algorithms. And then, we discuss the research direction of AQM in the future.

2. ACTIVE QUEUE MANAGEMENT

End-to-End TCP congestion control based on windows is very important for stability of Internet [1]. The traditional mechanisms of TCP employing an Additive Increase Multiplicative Decrease (AIMD) algorithm have been a critical factor in the robustness of the Internet. Modern implementations of TCP contain four intertwined algorithms: slow start, congestion avoidance, fast retransmit and fast recovery.

With more and more needs and developments of technology, the researchers begin to mean that if only depends on TCP congestion control, it is very difficult to meet complex need such as QoS. So, people begin to pay attention to the study of Active Queen Management. AQM scheme is critical technology based on routers congestion control and recommended by IETF (Internet Engineering Task Force). With AQM, the packet loss rate decreases, the end-to-end delay decreases and the network throughput increases [2,3]. AQM is the main way to resolve Internet congestion recently.

*The work described in this paper was fully supported by a grant from the project of 'Electronic Commerce Safe ', Nanjing College for Population Programme Management.

Before IETF put forward RED (Random Early Detection), Drop-Tail scheme based on FIFO (first-in-first-out) is only queue management of Internet. It is that, when buffer of routers is full, drop the packets follow through. Despite Drop-Tail is simple and easy to realize, its main defect is that it will bring obstruction and full queue, and cause many packets loss and the efficiency and function of Internet decrease. This urges IETF advises AQM on the end of router, which drops and marks a number of packets by some probability before queue is full, so that the source can response for congestion before buffer out-of range. The goal of AQM is controlling average queue length, reducing the packet loss rate, improving network throughput, avoiding network congestion and so on [4,5]. RED is the first AQM algorithm [6]. Besides RED, the other weighted AQM algorithms include: BLUE[7], PI[8], AVQ[9], REM[10], GREEN[11], CHOKe[12], etc.

3. RED

S.Floyd [6] brought forward RED in 1993. In order to overcome Drop-Tail defaults, RED inducts random early dropping packets mechanism for avoidance full queue. It utilizes queue EWMA (Exponentially Weighted Moving Average) to measure the congestion. It not only detects the impending congestion, but also removes the affect of gusty flows. RED algorithm (showing at fig.1) consists two parts:

1 Reach a new packet every time
2 Compute average queue length q
3 If $\min_{th} \le q \le \max_{th}$
4 Calculate probability p
5 Discard packets by probability p
6 If $\max_{th} \le q$
7 Discard packets

Fig.1. RED algorithm

(1) Calculate average queue length

RED adopts low-pass filter compute average queue length q. So, queue length increase caused by gusty flows and instant congestion will not affect average queue length increase. Computing average queue length by Exponential Weighted Moving Average formula as follow:

$$q = (1 - \omega) \times q + \omega \times q_{cur}$$

where the weight ω decides low-pass filter time constant and q_{cur} is current queue length. RED computing average queue length decides burst of routers queue flow contain.

(2) Calculate probability p of dropping packets

RED drops packets arriving routers, according to the computing probability p .RED makes use of three parameters $\min_{th}$, $\max_{th}$ and $\max_p$ computing probability p . (showing at figure 2)

$$p=\begin{cases} 0 & if \quad q < \min_{th} \\ \max_p \times (q-\min_{th})/(\max_{th}-\min_{th}) & if \quad \min_{th} \le q < \max_{th} \\ 1 & if \quad q \ge \max_{th} \end{cases} \quad (2)$$

where $\min_{th}$ is lower limit value of queue length, if average queue length is less-than low limit, packet will not be lost; $\max_{th}$ is upper limit of queue length; if average queue length is greater than this upper limit, the packets arriving routers will be lost; $\max_p$ is the maximum of the probability.

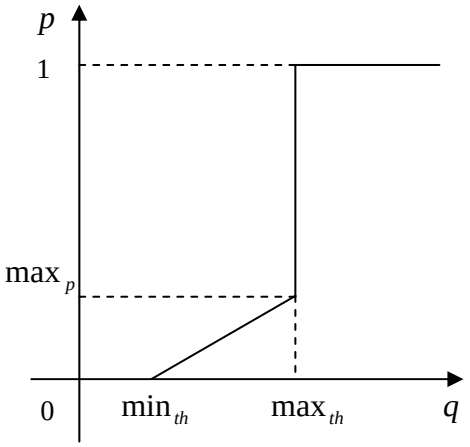


Fig.2. RED loss probability p

The main problem of RED is difficult to parameters configuration, and the improper configuration will lead to unsteadiness and behavior decline of Internet. So, despite new Cisco routers include RED option, RED is few used in practice.

4. ARED

When congestion is serious, RED must notify congestion information to enough sources so as to reduce load fully, avoid lose batching because of queue out-of-range. One of RED defaults is average queue length mostly depending on the load of Internet. If the load is gently, average queue length is approach to the minimum queue, and the system is unsteadiness. In order to solve above problem, Floyd put forward RED corrective mechanism, which is ARED.

The basic idea of ARED is through checking the average queue length change to decide RED behavior. That is drop more packets or select decrease the number of lose packets, so as to keep average queue length change between $\min_{th}$ and $\max_{th}$. In detail, if average queue length ranges near $\min_{th}$, it means that the congestion control algorithm is too radical, so, decrease $\max_p$, $\max_p = \max_p / a$. In the other way, if average queue length ranges near $\max_{th}$, that means congestion control algorithm is too conservative, then increase $\max_p$, $\max_p = \max_p \times b$ $(b > a > 1)$.

5. BLUE

BLUE performs queue management based on packet loss and link utilization. It maintains a marking probability p_m , either marks or drops the packets. The most contribution of BLUE is that realize congestion control making use of minor buffering area. But once losing packets, BLUE will increase packet loss probability relatively large, in order to create continuous packet loss, causing TCP traps in overtime, even lowing link utilization. BLUE has the problem of parameters configuration. BLUE algorithm is given below.

The BLUE algorithm:

Upon Packet loss (or $Q_{len} > L$) event:

$$If \quad ((now - last\_update) > freeze\_time)$$
$$p_m := p_m + \delta_1$$
$$Last\_update := now$$

Upon link idle event:

$$If \quad ((now - last\_update) > freeze\_time)$$
$$p_m := p_m - \delta_2$$
$$Last\_update := now$$

Marking probability, p_m , is also updated when the queue length exceeds a certain value in order to allow room to be left for transient bursts and to control the queue delay when the size of the buffer being used is large.

6. EM (RANDOM EARLY MARKING)

REM is a control mechanism based on flow measurement. It is a distributed algorithm. Its goal is to optimize the general function of network. Through dividing into groups marking, notify source end bandwidth price, asking source to adjust sending rate.

Different from RED through queue length measuring congestion, REM computes Price through matching rate and buffering, and calculates all the Price of congestion link accumulate one flow gather by exponential function. The common Price function is given below.

$$p_l(t+1) = [p_l(t) + \gamma(a_l(b_l(t) - b_l^*) + x_l(t) - c_l(t))]^+ \quad (4)$$

where $\gamma > 0$ and $a_l > 0$ are small constants and $[z]^+ = \max\{z, 0\}$. Here, $b_l(t)$ is the buffer occupancy of queue l in period t and $b_l^* \ge 0$ is target queue length, $x_l(t)$ is the aggregate input rate to queue l in period t , and $c_l(t)$ is the available bandwidth to queue l in period t . The difference $x_l(t) - c_l(t)$ measures rate mismatch and the difference $b_l(t) - b_l^*$ measures queue mismatch. When rates of input and output routers match, the queue length is $b_l(t) = b_l^*$, and the link utilization is $x_l(t) = c_l(t)$.

Precisely, suppose a packet traverses links

$l = 1.2 ..... L$ that have prices $p_l(t)$ in period t. Then the marking probability $m_l(t)$ at queue l in period t is:

$$m_l(t) = 1 - \phi^{-p_l(t)}. \quad (4)$$

where $\phi > 1$ is a constant. The end-to-end marking probability for the packet is then:

$$1 - \prod_{l=1}^{L} (1 - m_l(t)) = 1 - \phi^{-\sum_l p_l(t)} \quad (5)$$

Though REM works well on the state of steady, but the system may be not optimization when transient process and using limited buffering area.

7. CONCLUSIONS

Beside above algorithms, there are other main algorithms about congestion control. In 2001, Hollot, et al. put forward PI algorithm[8], which applies control theory nonlinear model in the link setting proportional-Integral controller, so as to adding system stability and adaptability. Kunniyur, et al. brought forward AVQ (Adaptive Virtual Queue) algorithm[9,13], which makes use of simple differential equation to adjust virtual queue capacity, having the aid of adjust utilization ratio factor and damping factor to realize the balance between higher utilization ratio and little queue length. In substance, it is a kind of early batching drop technology [14].

Wydrowski raised GREEN algorithm [11], which is a feedback control mechanism. Adjust congestion notification rate according to measured data arriving rate. Ao Tang, et al. put forward CHOKe (CHOose and Keep for Responsive Flows, CHOose and Kill for Unresponsive Flows) algorithm [12], which aims at protecting adaptive flow, punishes nonfittable flows. CHOKe takes on the benefit of RED basically, but increases extra expending a little.

Many AQM algorithms are based on queue control. Since 2001, Hollot proposed the TCP/AQM nonlinear model, many control algorithms based on queue, including of RED etc., which make use of control theory to setting parameters. Analyzing and designing algorithms are the hot points of AQM research now.

AQM has many merits, such as decreasing the number of packet loss in routers, offering lower delay for interactive serve, and avoiding deadlock. So, in the future, the develop direction is studying and exploring efficient AQM algorithms. Internet congestion avoidance and control is very important. In spite of many AQM algorithms being proposed by researchers, the algorithms' design and realization all face much compromise, such as throughput, response time, drop rates, and so on. It is impossible that there is one algorithm has the best function among all circumstances. So, study on AQM consists of reforming the existence algorithms, designing new algorithms and analyzing AQM algorithms etc.

REFERENCES

[1] Jacobson V., "Congestion Avoidance and Control," *ACM Computer Communication Review*, 1988, 18(4),pp.314-329.

[2] Braden, B., Clark, D., Crowcroft, J., et al. Recommendations on Queue Management and Congestion Avoidance in the Internet.RFC 2309, 1994. http://www.faqs.org/rfcs/rfc2309.html, 1994/2005-11.

[3] Floyd S., Jacobson V.,"On Traffic Phase Effects in Packet-Switched Gateways," *Internetworking: Research and Experience*,1992,3(3),pp.115-156.

[4] Li Ling,"Issues on the Active Queue Management," Ph.D. dissertation.,Fu Dan University, China, 2003

[5] Wang Bin, "TCP/IP Network Congestion Control Strategy Study,"Ph.D. dissertation,Zhe Jiang University,China,2004.

[6] Floyd S., Jacobson V., "Random Early Detection Gateways for Congestion Avoidance," *IEEE/ACM Transactions on Networking*, 1993,1(4):397-413

[7] Feng W., Kandlur D.et al, Blue: A New Class of Active Queue Management Algorithms. Technical Report, U. Michigan Cse-TR-387-99, http://www.eecs.umich.edu/~wuchang/blue/,1999/2005-11.

[8] Hollot C.V., Misra V.,et al,"On Designing Improved Controllers for AQM Routers Supporting TCP Flows.," In: Sengupta, B. ed,in *Proceedings of IEEE INFOCOM*. Anchorage,Alaska,USA: IEEE Communications Society,2001,PP.1726-1734.

[9] Kunniyur S.,Srikant R,"Analysis and Design of an Adaptive Virtual Queue(AVQ)Algorithm for Active Queue Management,"*ACM Computer Communication Review*,2001,31(4),PP.123-134.

[10] Athuraliya,S.,Li,V.H.,Low,S.H.,Yin,Q.REM, "Active Queue Management," *IEEE Network*, 2001, 15(3), PP.48-53.

[11] Wydrowski,B. and Zukerman,M. GREEN, "An Active Queue Management Algorithm for a self Managed Internet,"in *Proceedings of ICC 2002*, New York,Apr 2002,pp,2368-2372.

[12] Ao Tang,et al,"Understanding CHOKe,"in *Proceedings of IEEE Infocom*, San Francisco, CA,Apr 2003,pp.82-93.

[13] Abhishek Jain,Abhay Karandikar,Rahul Verma, "Adaptive prediction based approach for congestion estimation (APACE) in active queue management," *Computer Communications*,2004,27,pp.1647-1660.

[14] Ren Feng-Yuan,Lin Chuang,Liu Wei-Dong,"IP Network Congestion Control,"*Chinese Journal of Computer*,200326(9),pp.1025-1034(in Chinese).

Improvement of a Distributed Termination Detection Credit-Recovery Algorithm*

Yuxue Liu, Wenjing Li, Zhiping Liu
Guangxi Teachers Education University, Nanning, 530001,China
Email: xueyu775821@163.com

ABSTRACT

This paper introduces a distributed termination detection algorithm of credit-recovery algorithm, and improves the neck bottles of its credit value. It proposes an improved distributed termination algorithm model, and shows that the model is applicable to the decentralized and parallel computing by theoretical analysis and proof. The algorithm successfully improves load balancing, computing time and communicating complexity and other aspects.

Keywords: Distributed, Credit-Recovery Algorithm, Termination Detection

1. INTRODUCTION

In a distributed environment, whether the recognition calculation has already been concluded or not is an important issue to the termination detection. If the termination has already finished the calculation correctly, the calculation can get the final result. But something may be abnormal in the process of the calculating, such as the deadlock which would lead to terminating the calculation. At this time, it needs to judge the state of the termination, then re-counted. Usually, the usual judgment needs to satisfy the following distributional termination conditions at some time t: (1) at time t, regarding all process sets, there are the specific applications of the local termination conditions; (2) at time t, between the processes there are not the messages in the transmission [1].

2. CREDIT-RECOVERY ALGORITHM

In 1989, MATTERN proposed the Credit-Recovery Algorithm. The algorithm is a non-passive algorithm, and described as a "very smart" algorithm. The algorithm is as follows [2]:

Var $state_p$ (active, passive)
init if p= p_0 then active else passive;
$credit_p$: fraction init if p= p_0 then 1 else 0;
ret: fraction init 0; for p_0 only

S_p : { $state_p$ =active}
Begin send <message , $credit_p$ /2 >
End

R_p : (A message <message , c> has arrived at p)
Begin receive <message , c >;
$state_p$ =active;
$credit_p$ = $credit_p$ +c;
End

A_{p_0} : {A <return , c> message has arrived at p_0 }
Begin receive <return , c>;
return=return +c;
if return=1 then Announce;
End

From the above algorithm description we can know, the algorithm is activated only by P0, and others are the slave processes. The master process uses the centralized dispatch. The message transmission uses the approach that embeds the control message in the basic calculation information, in order to achieve the optimization. The methods of this termination detection are: (1) the master process has a fixed credit value 1.When a process is activated by a message, this message gives its own credit value to the process, and the process is allowed to point to the root node of the tree which this message is in. When the process completes its tasks, it will send the credit value to the root node, where the process is. Then the root node adds this value to its own return value. (2) The message transmission mode of the process: When an activated process sends a message, its credit value is averaged two parts. One part appoints itself and the other appoints this message. Then the activated process inserts its root node symbol to this message. When an activated process receives the basic message, it returns the message credit value to the root node where the message is.

However, this algorithm has a distinct problem that the credit value is divided into two in average. The method has positive number credit value that smallest is unable to be divided again. But in the one divided into two parts, it can have the floating number operation. The summation of the floating numbers, which are returned to the return value variable, is uncertain equal to the original fixture 1. This inequality can easily generate errors, thus cause to the failure of the terminate detection. Therefore, this article makes some improvements in the Credit-Recovery Algorithm, in order to avoid generating the floating point calculation in the basic message and the duty assignment process and so on. These improvements can improve and optimize the termination detection algorithm.

3. CREDIT-RECOVERY ALGORITHM IMPROVEMENT

The improved algorithm, which is based on Credit-Recovery algorithm, proposes a thought that founds on the distributed system in decentralized parallel computation and the precise termination computation in the detection. The basic thought is: using the function division technology and according to the function, the whole procedure is divided into the mutual independence function module set, which is recorded as Q. Each function module is recorded as Pi(i=1,2,…,n).And the credit value of each Pi's root node is assigned the initial value 1,credit=1.Suppose a constant named count which is the number of counting the functional modules, and its initial value is 0. Whether the judgment calculation is finished or not, is according to the summation of the credit values which return, when Pi terminates the computing. This sum is saved in the

* Supported by Department of Education of Guangxi zhuang Autonomous Regional (0626120) and Guangxi Teachers Education University (0604A005).

constant count, count=count + credit (Pi). Every execution time, the process must examine that whether the value of count is equal to the value n. If the result is equal, this algorithm terminates. Otherwise, it continues to carry out.

Each functional module Pi uses the tree structure and undulation algorithm to carry on the termination detection. Its specific ideas are as follows:

Each functional module Pi (i = 1,2, ..., n) supposes the root node named Pi(0).The credit value of Pi(0) is 1.The original return value of Pi(0) is 0,which is used to statistic the number of the processes that have finished the computation. Its root symbol is marked as i, which is the subscript of Pi. The variable count (i) is to count the process number and the transmittal basic message number. In the improvement algorithm, the credit values of all the basic messages and the active processes are 1.This has guaranteed that this algorithm can't generate the negative number and the floating number possibility.

Regarding each Pi tree, if its count (i)'s value of the root node Pi (0) is equal to the value of return (i), then it means that in this tree, there aren't the transmitting basic messages and the active processes. In a word, this Pi tree has already terminated the computation. At the same time, we should send the credit value of Pi (0) to the constant count.

In summary, this article summarizes several rules from the improved algorithm. As follows:

Rule1: When the count value and the n value is equal, namely count=n, it shows that the entire calculation has terminated, and obtained the final results. The variable n is the number of the division function modules, and the constant count is the number of the function modules which have been calculated successfully.

Rule2: When count(i)=return(i), it indicates that the termination detection of the Pi tree that has finished. The return (i) expresses the sum of the return values in the Pi tree. Meanwhile count=count +credit (Pi), shows that a function module finishes its computation.

Rule3: When a process becomes passive, it would send the credit value to the root node of the Pi tree. The root node adds this credit value to its own return (i) value.

Rule4: When a process is activated by a message, the process credit value is equal to the message's credit value (this message's credit value is assigned to the credit value of the process), namely the value is 1. According to the message with the message-signs, the process is inserted to the Pi tree, and connected under its father process. The root label ID(i) also adds to the control information of this process according to the message's control information. Then count(i)=count(i)+1.

When a process is activated, there is a special situation that the activated process has already belonged to a Pi tree. At this case, we remove it from the original Pi tree. Then its root label ID (i) changes into ID (j). And this process is connected to the Pj tree.

Rule5: When an activated process sends a message, the root node label ID(i) of the Pi tree will embed in the message. The message is given a credit value 1, and count(i)=count(i)+1.

Rule6: When an active process receives a message, the process returns the message credit value to the return(i) value of Pi tree's root node.

The improved algorithm, which is described by the category similar C language, is as follows:

```
Var    contant int count=n;
        int count(i)=0;
        int return(i)=0;
        int ID(i)=i;
        int credit(Pi)=1;
       int P(i,j);
       int credit(i,j);
       int ID(i);
       state(Pi):(active,passive);
       state(P(i,j)): if P(i,j)∈Pi then active else passive;
       boolean terminate（Pi）=0;
S:{state(Pi)=active}
     {   send<message,ID(i)>;
         credit(i,j)=1;
         count(i)=count(i)+1;
      }
R:{A message<message,ID(i)> has arrived at P(i,j)}
     {   if state(p(i,j))=passive
                  then {   state(p(i,j)=active;
                           credit(i,j)=1;
                           ID(j)=i;
                           count(i)=count(i)+1;
                        }
                  else   return(i)=return(i)+credit(i,j);
        }
     T(Pi):{state(Pi)=active};
        {    if (return(i)==count(i))
                then   { state(Pi)=passive;
                         count=count+credit(i);
                         terminate(Pi)=1;
                         }
        }
T:{ if (count==n)   then   terminate;}
```

4. THE ALGORITHM PROOF

The improved algorithm is a correct distributed termination detection algorithm.

Prove: Supposed T is all the processes and the basic messages of the Pi tree. Since the improved algorithm is accord with the rules from 2 to 6, and some other basic conditions. All the credit values of the processes and the messages in the Pi tree are 1. And these values are also invariable in the procedure. Count(i) counts the number of the messages and the number of the processes in the computing process. When the message transmissions end and the process computations finish, they return their credit values to the return(i) value of the root node, namely, return(i) is the sum of the number of the credit values of the messages and the processes. When count(i) and return(i) is equal, it means that there aren't the transmitting messages and the active processes, we can obtain the conclusion that the Pi tree has terminated computation. The value of termination(Pi) marks 1, namely, terminate(Pi)=1. Similarly other trees can be calculated the termination.

When a Pi tree terminates computing, its credit value must be returned to the constant count, namely, count=count+ credit(Pi).While the termination detection finishes, the program must examine the count value whether it is equal to n. If the result is true, it means that the entire computing has already

finished correctly. Therefore it could obtain the final results.

When a Pi tree's root node has detected the own computing termination, but it is activated again by a message which another Pj tree sends. In this time, the root node of the Pi tree is connected to the Pj tree. But it does not affect the termination status of Pi tree. In other words, when the terminate value of Pi tree is given the value 1, it will never change again.

In conclusion, the improved algorithm is a correct distributed termination detection algorithm.

5. PERFORMANCE ANALYSIS

The Credit-Recovery algorithm is a non-undulation algorithm. Its distinct problem is that it generates a minimum credit value, which is not any longer divided, and produces the float number. Because this algorithm uses the method that one credit value is averaged to two parts.

In the improved algorithm, it uses the lock-up credit value method, and the lock-up value is 1.This method can avoid the smallest positive number and the float number. Unlike the Credit-Recovery algorithm, the improved algorithm uses the multi-function modules method, namely, the entire program is divided into several function modules. And it enables the parallel. So the improved algorithm is better fit for the distributed computing. In the improved algorithm, the algorithm uses the tree structure method. In this tree, the nodes get the label of the root node by the message's transmission. And they need not understand other nodes' messages. Thus, it is more suitable for the distributed system. And it increases the utilization of the system resources, and also saves the message transmission time. It is a distributional termination detection which is simple and easy to achieve.

6. CONCLUSIONS

In a distributed environment, the termination detection is an important part of the distributed computing. This article proposes the improved termination detection algorithm in terms of the Credit-Recovery algorithm's insufficiency. This improved algorithm, which can achieve non-central parallel computing termination detection, is highly effective, more precise and adapts the distributional non-centralized algorithm and so on.

REFERENCES

[1] Barry Wilkinson, Michael Allen. *Parallel Programming: Techniques and Applications Using Networked Workstations and Parallel Computers*.Xinda Lu Trans. Beijing: China Machine Press,2002(in Chinese).

[2] Xuming Liu, Yunlin Su. "Improvement of a Distributed Termination Detection Algorithm". *Software Journal*, 2003, 14 (1) : 49~53.

[3] Mattern F. "Global quiescence detection based on credit distribution and recovery". *Information Processing Letters*, 1989, 30(4):195~200.

[4] Chang Gu, Wenjie Liu. "Cycle Termination Detection Algorithm for Protecting". *Computer applications*. 2006. 26 (2).

[5] Hong Zhou, Shumin Diao. "The New Distributional Algorithm Research". *Jiamusi University Journal (Natural Science)*. 2006. 24 (3).

[6] Lianwei Zhao, Siwei Luo. "Binary Tree Dynamic Load Balancing Methods". *Computer applications*. 2003. 23 (7).

Network/Web Security

OpenID, an Open Digital Identity Management and Authentication Framework

Runda Liu, Juanle Wang, Jia Du
Institute of Geographic Sciences and Natural Resources Research, CAS
Graduate School of Chinese Academy of Sciences
Beijing, 100101
Email: liurd.05b@igsnrr.ac.cn

ABSTRACT

OpenID is an Open Digital Identity Management and Authentication Framework on the Internet, Compared with traditional digital identity management systems, it has main characteristics of URI/URL based, decentralized management and user centric philosophy. In the web 2.0 era with flourishing web applications and Internet services, as a new technology, OpenID reduces accounts registration and identity management errands for Internet users, it provides a single sign on mechanism as well. Focused on the 3 characteristics of OpenID, this paper introduces briefly its authentication mechanism, applications and developments; finally, some weak points of current OpenID specification and concerns are discussed.

Keywords: OpenID, Authentication, Digital Identification

1. CURRENT STATUS OF INTERNET DIGITAL IDENTITY MANAGEMENT

The Internet is evolving rapidly towards a so called web 2.0 era[1] in which web applications and Internet services are flourishing. The existing Internet architecture, based on the IP protocol, was designed with simplicity in mind, it provides an effective way to connect devices but does not concern itself with whom or what is being networked. As a result, Internet users wishing to take part in private communications or transactions ordinarily have to establish their identities by manually creating unique accounts at each Internet service[2]. Identities or accounts registered for certain web applications or Internet services are called Digital Identity.

While web applications or Internet services need authentication to use, websites on which web applications or Internet services hosted need separate user identity management and authentication systems to function, this bring many trouble not only to the websites building, but also to internet users who use these sites[3], to name a few:

- ✧ User has to register accounts in different websites to use the services they provide
- ✧ Different username/password pairs should be employed in case of security hole of Internet services
- ✧ Internet users cannot always register their most wanted accounts in every sites
- ✧ Account management is an errand for Internet users, for most users, username and password for less used websites are usually forgotten

Current digital identity management and authentication framework on the Internet start hindering the progress of Internet services, therefore, an Internet based universal digital identity management system is of high demand. As a result, many digital identity management solutions and authentication frameworks emerged, e.g. Microsoft's Live Passport, Google Account, SAML authentication, Cardspace and OpenID, etc. Among these solutions, OpenID [21] is a light weighted, open standard solution; it solves many problems that facing traditional identity management and authentication systems including items listed above.

2. OPENID AUTHENTICATION FRAMEWORK

OpenID is an open, decentralized, free framework for user-centric digital identity [4], its logo is shown in Fig.1. The OpenID 1.0 specification is originally drafted by Six Apart's chief architect Brad Fitzpatrick in 2005[5]; OpenID authentication came from the idea of authenticating to different blogs using one single digital identity to write comments, finally it developed into a more widely used digital identity management system.

Fig.1. OpenID Logo

A typical OpenID authentication process involves 4 parties: End User, Identity Page, Relying Party and Identity Provider:

End User: Internet user who attempts to authenticate to web applications or Internet services using an OpenID, end user also refers to user agent such as a web browser.

Identity Page: Also called OpenID Identity, Identity URL, refers to the identity URI/URL that is used as an OpenID during an authentication process or the file located in that URL. The purpose of OpenID authentication is to prove the Identity Page provided is owned by the end user.

Relying Party, RP: Also called OpenID Customer, mostly, it refers to the OpenID Enabled website, web application or Internet service.

Identity Provider, IDP: Also called OpenID service provider, OpenID authentication server or OpenID server. It's the place where user profile is hosted. IDP provides identity authentication service for RP by encrypted communications.

1) Relying Party associates with IDP (Option 1): In order to communicate securely with the OpenID server, the RP gets an association with the IDP discovered in step 2, using an existing association if it is available, otherwise visiting the OpenID server and using Diffie-Hellman to negotiate a shared secret with which to sign communication. A RP unable to store state uses "dumb mode" which does not perform this step, and instead uses step 7.
2) Relying Party redirects the user to the IDP: The OpenID server URL accepts a query, containing all the information the server needs to check the user's identity and redirect the user back to the RP. The OpenID server checks the authentication of the user. If the user is signed in (has an auth cookie) and has already authorized sending their identity to the RP, step 5 may be skipped.
3) End User Authenticates to IDP: The user authenticates to the IDP with a cookie or a username and password, and the IDP asks the end user for permission to send their identity information to the RP.
4) IDP redirects the End User back to the Relying Party: The

Relying Party parses the OpenID server's response (which is appended to the return-to URL the Relying Party sent) and verifies it using the association, or in the case of dumb mode proceeds to step 7.

5) Relying Party verifies the response with the IDP (option 2): Communicating directly with the Identity Provider, the dumb mode Relying Party checks the response received via the User Agent in the redirect.

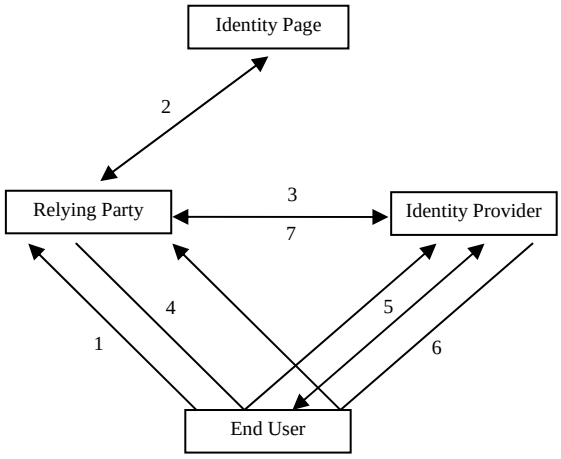


Fig.2. Diagram of OpenID Authentication Process[6]

3. OPENID AND ITS MAIN CHARACTERISTICS

What makes OpenID a buzz in authentication and identity management solutions is that there are many innovative features of OpenID. Among them, URL as digital identity, decentralized management and user centric implementation makes the big differences from other digital identity management systems.

3.1 URL as Digital Identity

The most primitive digital identity registration method is to let Internet users to choose combination of letter and number as their user names. Later, Internet service providers let users to register accounts with their email addresses for the reason of simplicity. Different from the above two methods, OpenID uses a simple URI/URL that user own as digital identity to log into OpenID enabled websites.

When end user click the login button in an OpenID enabled website after input its OpenID URL, what an OpenID authentication mechanism do is to verify that the user owns this URL. Password or certificate for an OpenID login is safely stored in the IDP that user chose, during the process of authentication, there is no passwords transfer among different parties. the key to login an OpenID enabled website is just a URL, owning an OpenID, users get fast access privileges to all OpenID enabled websites and not need to suffer from the endless boring registration and login process any more[7].

3.2 Decentralized Digital Identity Management

By implementation, OpenID separates identity management systems from Internet services. Different from most traditional digital authentication systems in the most basic point is that OpenID identity management is actually a decentralized system. Users of OpenID consumers come from different OpenID providers, users hosted by one OpenID service provider are able to authenticate to different Internet services. Users can choose any OpenID service provider as they wish, if needed, they can setup their own OpenID authentication servers [8]. As a result, when an opened enabled website is out of service, the digital identity that user used to login will not be affected in other RPs.

After a URL owner registered in an IDP, he can use the authentication and identity management services provided by the server, If the OpenID service provider is out of service, he can start use a new OpenID service, what he need to do is shift IDP by changing some parameters. That is to say, if a user owns a URL as OpenID, he is always the owner of this OpenID digital identity and this is the merit that comes from the decentralized management style.

3.3 User Centric

The feature of user centric is a main difference of OpenID from other traditional digital management system. User centric means user profiles on the OpenID server is the centre of Internet users' online being [9], OpenID end user can actually manage and control the spread and share of its Personally Identifiable Information(PII) or personal profile.

When a URL owner registering in an IDP, a detailed personal profile is needed, this information will not be shared immediately by the web applications or Internet services user authenticate to using OpenID. In general, when login to a new OpenID enabled web application or Internet service, the PII transfer is required, because most web applications need to know something about its end user by create brief profiles in background. By the OpenID Attribute Exchange Specification, user can control the share level of its personal profile, for example, in some case, only user's true name, address and telephone number is able to shared, etc, some OpenID service, like Verisign, can create different "Trust Profile" from the user's PII, and provide different OpenID enable website with different "Trust Profile" [10].

4. THE DEVELOPMENT OF OPENID AND ITS APPLICATIONS & DISCUSSIONS

4.1 Adoption of OpenID

OpenID is under active development, until the end of 2006, a bunch of OpenID Identity providers emerged: e.g. MyOpenID.com and Livejournal.com; Even Verisign starts its OpenID based Personal Identity Provider service, PIP[11]; some traditional network service providers also provide or willing to provide OpenID supports, for example, AOL started provide OpenID service, every AOL/AIM user can get a http://openid.aol.com/<screenName> URL as OpenID; Bill Gates declared in the "RSA security summit" in 2007 that Microsoft will support WS-* and the decentralized OpenID digital identity protocol[12]; idproxy.net was setup to bridge yahoo ID system with OpenID specification to provide OpenID authentication service[13]. According to a statistics, currently, there are as many as 1,200 sites offer some sort of OpenID services, reaching a potential 75 million people worldwide. Those figures could balloon to 15,000 sites and 250 million people this year [14].

In the Relaying Party side, many web applications started support OpenID login, e.g. Zooomr.com and Technorati.com; the creator of Digg.com Kevin Rose spoke in the "Future of Web Apps 2007" that Digg.com will use OpenID as its authentication system. OpenID also gain supports from third party tools and applications, for example, WordPress plugins used for OpenID login to post comments are ready for download; OpenID plugins for different wiki systems have been developed, e.g. OpenID plugin for DokuWiki can be found in Splitbrain.org[15]. Client tools start support OpenID as well, e.g. the under developed firefox version 3.0 software

will provide OpenID support.

As for the OpenID specification development, its current version is 1.1, the OpenID 2.0 specification is almost out, version 2.0 added Yadis support in the identity service information discovery, more security concerns are added; new features like public and private identity presentation is added. OpenID 2.0 support i-names as well, PII transfer and OpenID data transmission functionalities will be improved greatly in Version 2.0, what's more, an open interface is a key design idea of version 2.0.

4.2 OpenID Philosophy

OpenID is open, nobody should own it. Nobody's planning on making any money from it. The goal is to release every part of it under the most liberal licenses possible, so there's no money or licensing or registering required playing. It benefits the community as a whole if something like it exists[8].

OpenID is a brand new Internet based digital identity management framework, OpenID identity provider itself is not to compete for user resources with web applications or Internet services, nor does it try to replace current web applications' user database. The philosophy of OpenID is actually try to implement a user centric digital identity management on top of current user management system and share user resources across cooperate domain. The share of user resources facilitates user register and authentication process.

Under the OpenID framework, RPs are not to solicit user registration in any ways, but to put more efforts on how to better their services to gain visits from users, the registered user resources is already there, web applications or Internet services do not have to start from scratch. For users, when login to an IDP, they can visit any other RPs without further login processes, user is actually having a universal passport, login one place, login everywhere; this is the so called Single Sign On(SSO), compared with the old "Passport" service, SSO service provided by OpenID transcend the enterprise domain, and also, the open and free characteristics are what Live Passport or Google Account currently cannot offer.

4.3 Weakness and Thoughts

Although many merits and good points, OpenID specification is far from full fledged, for example, the current version 1.1 of OpenID specification doesn't support grace logout mechanism, and in some situations, the speed and stability need to be improved. Below are some of the main concerns and weakness of current OpenID implementation [16-19].

1) *Privacy:* User centric OpenID makes digital identity management the heart of Internet user's online life, while general public have difficulties to setup their own OpenID servers, thus they have to choose IDPs to use, this will bring privacy concern for users, for example, if Internet user uses an OpenID identity provider for all of the logins, that IDP knows exactly which sites the user visit, and which companies user shop from, etc, that kind of information is very valuable to marketer and likely to get sold or stolen.
2) *Security:* To a lesser extent, OpenID promotes identity theft, partly, this is due to its user centric feature, while OpenID service provider becomes the main user profile hosting place, it exposes Internet user to theft, deception and spam, and user is more likely get targeted. Also, because of the open source feature of OpenID, every body can start an IDP, this will cause security problems for OpenID enabled sites and services.
3) *Popularity and Buy-in:* OpenID is useless unless everyone buys into it. Currently, there are too many providers, not enough consumers[20], then even if it is an amazing technology, if it is not accepted by Internet users, it won't prevail. A merit of OpenID is that it helps people manage digital identity and control the share of PII, but while "digital identity" is actually a virtual concept, it's not a really item, if not many people pays attention to it, then it will not exist at all.
4) *Corporate Control:* The use of OpenID is sometimes confined in a corporate domain; it is used as a single sign-on solution and to gather user data more easily. Corporate control exists because the fact that to verify and judge which OpenID identity provider is safe and trustworthy is very difficult. Even, some application websites will only accept the OpenID provider they trust to allow, and may refuse other small OpenID provider service. Corporate control defeats the purpose of OpenID, makes the philosophy of OpenID meaningless.

Many other concerns and thoughts were discussed among the OpenID community, however, there are also many solutions and proposals that tackle these weakness, for example, Replying party must allow users to "link" their existing accounts with OpenID; public domain Relying Party should not limit the choose of OpenID service provider etc. With the community support and development, some of these ideas have been implemented in OpenID software released, OpenID specification are also take its weakness into consideration and make OpenID more stable and reliable.

5. CONCLUSIONS

Web applications and Internet services are evolving in a never seen speed; the need for a universal digital identity management on the Internet is becoming more and more urgent. OpenID provides a brand new framework for Internet based digital identity management, the characteristics of URI/URL based, decentralized and user centric makes OpenID a very promising technology.

However, OpenID's final goal is to reach a widely use, if not, it will lose its reason to exist. After more than 2 years of development, OpenID has developed from its simple authentication function to a more accepted digital identity management and authentication framework. Nowadays, many websites and web applications support or will support OpenID. Although many other thoughts and arguments towards it, with its easy and concise authentication framework, OpenID maybe a candidate among digital infrastructures for the future Internet applications.

REFERENCES

[1] LIU Run-da, L.S.L.H.-l., *Web2.0 and its Impacts On the Internet. Modern Computer.*
[2] Tsui, W., *Digital Identity Management on the Internet*. 2006.
[3] Yan, M., *Web2.0, SSO & OpenID*. 2006, http://xerdoc.com/blog/archives/225.html.
[4] *What's is Openid*: www.openid.net.
[5] David Recordon, D.R., *OpenID 2.0: A Platform for User-Centric Identity Management*. 2006.
[6] Arneson, D., *OpenID Protocol*. 2006, http://www.openidenabled.com/openid/openid-protocol.
[7] Yan, X., *Enable Your OpenID Soon*. 2006: http://herock.net/archives/000187.htm.
[8] Ellin, B., *About OpenID*. 2006, www.openidenabled.com: http://www.openidenabled.com/openid/about-openid.

[9] Gaal, R., *Making OpenID your on ly online profile: Alpha Dash*: http://www.53miles.com/archives/making-openid-your-only-online-profile-alpha-dash.
[10] Xiaoyun, Z., *verisign Personal Identity Provider service*. 2006: http://www.klogs.org/2006/06/18/pip.htm.
[11] *OpenID for the Semantic Web* 2006, Geospatial Semantic Web Blog: http://www.geospatialsemanticweb.com/2006/10/25/openid-for-the-semantic-web.
[12] *Gates Says Microsoft Will Support OpenID*. 2007: http://yro.slashdot.org/article.pl?sid=07/02/06/2152214&from=rss.
[13] Xiaoyun, Z., *Microsoft support OpenID*: http://www.klogs.org/2007/02/08/.
[14] Swartz, J., *Technology cuts down on Web registrations*. 2007: http://www.usatoday.com/tech/webguide/internetlife/2007-03-15-openid_N.htm?csp=34.
[15] Xiao-fei, G., *2007, the year of OpenID*. 2007: http://if20.net/2007/01/12/2007-the-year-of-openid/.
[16] *Why OpenID will fail. AKA OpenID disinformation time.*, the best things in life are free: http://scotthadfield.ca.
[17] Migurski, M., *openID*: http://mike.teczno.com/notes/openid.html.
[18] Migurski, M., *more against openID*: http://mike.teczno.com/notes/openid-again.html.
[19] *Why OpenID is Meaningless*: http://openids.cn.
[20] Cubrilovic., N., *OpenID: Too many providers, not enough consumers*: http://www.nik.com.au/archives/2007/03/12/openid-too-many-providers-not-enough-consumers/.
[21] www.openid.net

Homomorphic Encryption Based on Fraction*

Ping Zhu [1,2]
[1] School of Computer, Wuhan University
Wuhan, Hubei, 430072, China
[2] School of Information,Zhongnan University of Economics and Law
Wuhan, Hubei, 430062, China
Email: zhuping@znufe.edu.cn

ABSTRACT

The homomorphic encryption can be used in many useful applications including multi-party computation, electronic voting, and database encryption. The existing homomorphic encryption is based on ring of the integer, and the possible operators are restricted to addition and multiplication only. In this paper, two new operations are defined -- Similar Modular and Fraction Modular. Base on the Similar Modular and Fraction Modular, the number sets of the homomorphic encryption is extended to the rational, and the possible operators are extended to addition, subtraction, multiplication and division. Our new approach provides a practical ways of implementation because of the extension of the operators and the number sets.

Keywords: Private Homomorphism, Similar Modular, Fraction Modular; Homomorphic Encryption.

1. INTRODUCTION

With the development of informationization and digitalization, the importance of the security and secrecy of information is increasingly recognized. Ordinary encryption can't compute the ciphertext data, however, homomorphic encryption can do it and furthermore encrypt operation value automatically. Therefore, homomorphic encryption can be widely used in multi-party computation, electronic voting, and mobile cryptography[1-3]. In this paper, the interrelated technology of homomorphic encryption is recalled. A new operation, similar modular, is defined. Homomorphic encryption is realized in the range of the rational based on similar modular operation. This mechanism can process arithmetical operation of addition, subtraction, multiplication and division to the ciphertext data.

The remainder of this paper is organized in the following way: In Section 2 we introduce the idea of privacy homomorphism. In Section 3 homomorphic encryption of the integer is discussed. In Section 4 we discuss the details of homomorphic encryption of the rational. In Sections 5 we briefly give conclusion and some future works for our approach.

2. PRIVACY HOMOMORPHISM

The homomorphic encryption presented in this paper is based on a concept that may be traced back to the article on privacy homomorphisms by Rivest, Adleman, and Dertouzos[4]. The homomorphic encryption is a subset of privacy homomorphisms. The concept behind privacy homomorphism is to improve security by allowing direct computation on encrypted data without decryption. Rivest, Adleman and Dertouzos defined privacy homomorphism as follows：

Let S be a set, and S' a possibly different set with the same cardinality as S. Let D : S→ S' be bijective. D is the decryption function, the encryption function is E. Assign an algebraic system for plaintext operations by:

$$U=< S; f_1,...,f_k; P_1,...,P_l; s_1,...,s_m >$$

Where the f_i is operator, the P_i is predicate, and the s_i is distinct constant. Assign converse compution of U with encrypted data by:

$$C=< S'; f_1',...,f_k'; P_1',...,P_l'; s_1',...,s_m' >$$

Where the f_i' , P_i' s_i' are the encrypted version of f_i , P_i , s_i respectively. The mapping D is called a privacy homomorphism if it satisfies the following conditions:

① $\forall i(a,b,c,...)(f_i'(a,b,...)=c \Rightarrow f_i(D(a),D(b),...)=D(c))$

② $\forall i(a,b,...)(P_i'(a,b,...) \equiv P_i(D(a),D(b),...))$

③ $D(s_i')=s_i$

In order for C and D to be of any use as a protection, the following additional constraints should be satisfied:

① D and E are easy to compute.

② The functions f_i' and predicates p_i' in C are efficiently computable.

③ E is a non-expanding cipher or an expanding cipher whose cryptotext has a representation only marginally larger than the corresponding plaintext.

④ The operations and predicates in C should not be sufficient to yield an efficient computation of D.

Additionally, E and D must resist ciphertext only and chosen plaintext attacks. If a cryptographical system such as this could have existed, it would have been applicable for almost all problems which secure multiparty computations are designed to solve. Privacy homomorphisms were originally conceived as a method of processing encrypted data. In more recent times, it has been proposed as a principle underlying encrypted computation [5, 6].

3. HOMOMORPHIC ENCRYPTION OF THE INTEGER

Sander and Tschudin defined additive-multiplicative homomorphism of the integer [7-9], which is a kind of privacy homomorphism. Additive-Multiplicative homomorphism ensures that the computation result on two encrypted values is exactly the same as the encrypted result of the same computation on two unencrypted values. Sander and Tschudin's mobile cryptography uses HOMOMORPHIC ENCRYPTION for its implementation, but there are some drawbacks. First, no single cryptosystem is found to be

* Supported by the National Natural Science Foundation of China (90104005).

additively, multiplicatively and mixed multiplicatively homomorphic. Second, only some limited classes of functions (polynomial and rational functions) are proved to be compatible with the HOMOMORPHIC ENCRYPTION. Here, we describe the properties of homomorphic encryption that we need for securing computation from the work of Sander and Tschudin:

Let R and S be sets. We call an (encryption) function

$E : R \rightarrow S$

① **Additively homomorphic** if there is an efficient algorithm **PLUS** to compute $E(x+y)$ from $E(x)$ and $E(y)$ that does not reveal x and y.

② **Multiplicatively homomorphic** if there is an efficient algorithm **MULT** to compute $E(xy)$ from $E(x)$ and $E(y)$ that does not reveal x and y.

③ **Mixed-multiplicatively homomorphic** if there is an efficient algorithm **MIXEDMULT** to compute $E(xy)$ from $E(x)$ and y that does not reveal x.

The homomorphic encryption that meets the three properties allow only two types of operators: addition and multiplication. One thing to note is that there is one-to-many relationship, which implies that a single plaintext message, x, can have multiple ciphertext messages of $E(x)$ (i.e., although $E_1(x) \neq E_2(x)$, $D(E_1(x)) = D(E_2(x))$ is true for a plaintext message x). Another point to note is that there should be only a few elements that satisfy the last property (mixed-multiplicativity), otherwise the last property and the second property yield an anomaly, $y = E(y)$. Thus, in integers, only one integer (a multiplicative identity, $x = 1$) should satisfy the last property, $E(xy) = E(x)y$, to avoid the anomaly.

Since common addition and multiplication are homomorphic of the integer, homomorphic encryption of the integer is very easy. Let R and S be sets of the integer, R is plaintext data, S is ciphertext data. a∈R and b∈R, E be a encryption function between them: $E : R \rightarrow S$. The algorithm PLUS is called additively homomorphic if it satisfies the following conditions:

$$E(a+b)=PLUS(E(a), E(b))$$

The algorithm MULT is called multiplicativity homomorphic if it satisfies the following conditions:

$$E(a\times b)=MULT(E(a), E(b))$$

In this way there E(a+b) and E(a×b) can be computed from E(a) and E(b) that does not reveal a and b. In the plaintext code PR, the additions are replaced the algorithm PLUS, the multiplications are covered for MULT, the ciphertext code PR_E is build by the PR. The PR_E is executed on the remote host, the computing result of the PR_E is encrypted automatically. The rational result can be gained by decryption.

The new cryptosystem uses a large number, n, such that $n = p \times q$, where p and q are large prime numbers. Let $Z_p = \{x \mid x \le p\}$ be the set of original plaintext messages, $Z_n = \{x \mid x < n\}$ be the set of ciphertext message and $Q_p = \{a \mid a \notin Z_p\}$ be a set of encryption *clues*. The types of operations defined are addition and multiplication on Z_p. The encryption and decryption algorithms are as follows:

Encryption Given $x \in Z_p$, pick a random number a in Q_p such that $x = a \bmod p$. Compute the encrypted value $y = E_p(x) = a \bmod n$. This can be accomplished by picking a random r and creating $a = x + rp$.

Decryption Given $y = E_p(x) \in Z_n$, use the key p to recover $x = D_p(y) = y \bmod p$.

Example Let p=29,q=23,n= $p \times q$=667 and the values, x_1=7 where $E(x_1)=(7+28\times29) \bmod (29\times23) = 152$, and x_2=3 where $E(x_2)=(3+40\times29) \bmod (29\times23)=496$.

$E(x_1+x_2)=PLUS(E(x_1),E(x_2))=E(x_1)+E(x_2)= 152+496=648$

$E(x_1\times x_2)= MULT(E(x_1),E(x_2))$

$= E(x_1)\times E(x_2)= 152\times496=75392$

Decrypting $E(x_1+x_2)$ and $E(x_1\times x_2)$ yields,

$D(E(x_1+x_2))= 648 \bmod 29 =10= x_1+x_2$

$D(E(x_1\times x_2))= 75392 \bmod 29 =21= x_1\times x_2$

4. HOMOMORPHIC ENCRYPTION OF THE RATIONAL

Since homomorphic encryption is produced, the last word is homomorphic encryption of the integer, and the possible operators are restricted to addition and multiplication[10]. In this paper homomorphic encryption of the rational is proposed, the possible operators are extended to addition, multiplication, subtraction and division. Our new approach provides some practical ways for implementing homomorphic encryption, and this new approach will encrypt data in a way that enables direct computation on encrypted data without decryption.

4.1 Additively Homomorphic

To discuss the additively homomorphic of the rational, the new operation is defined in our approach, called similar modular, expressing as "smod" in short.

Definition 1: smod is a binary operation, it is a rational vs a plus integer to compute modular. smod is yielded as fellow:

$$smod(m,p)=\begin{cases} mod(m,p) & m\ge 0 \\ -(mod(|m|,p)) & m<0 \end{cases}$$

where m is a rational, and where p is a large plus prime number, and where mod() is common modular-operation. The security is not damaged where p is restricted an integer greater-than zero.

Example: smod (9.8,4) = 1.8,

smod (-9.8,4) = -1.8

Some properties of smod are alike with properties common mod.

Because subtraction can be expressed as a plus rational adds on a minus rational, additively homomorphic of the rational is only discussed. The encryption and decryption algorithms are as follows:

Encryption:

① The algorithm of additively homomorphic uses a large number, n, such that $n = p \times q$, where p and q are large security prime numbers. Let $Z_p = \{x \mid x \le p\}$ be the set of original plaintext messages, $Z_n = \{x \mid x < n\}$ be the set of ciphertext message.

② Given $x \in Z_p$, Compute the encrypted value $y = E_p(x) =$ smod((x+sign(x)×rand()×p),n). where rand() yields a random plus integer, and where sign(x) produces a plus or minus symbol like x.

③ Given $x_1 \in Z_p$ and $x_2 \in Z_p$, to compute x_1+x_2, first of all calculating $y_1= E_p(x_1)$ and $y_2= E_p(x_2)$ according to ②.

④ If $|x_1|-|x_2|\ge 0$, then $|y_1|-|y_2|\ge 0$, otherwise return ③ to recalculate y_1 or y_2. as far as the condition is satisfied.

⑤ Calculating y_1+y_2, the result is encrypted automatically.

Decryption Given $y = E_p(x) \in Z_n$, use the key p to recover $x = D_p(y) =$ smod(y,p).

Example(Addition) Let p=19,q=17,n= p×q= 323 and the values,x_1=2.5

where $y_1= E_p(x_1)$=smod((2.5+23×19),323)=116.5.

and x_2= -4.15 where $y_2= E_p(x_2)$=smod((-4.15-31×19),323)

= -270.15.

$y_1+y_2= E_p(x_1)+ E_p(x_2)= 116.5+(-270.15)= -153.65$
Decrypting -153.65 yields,
$D_p(-153.65)=\text{smod}(-153.65,19)= -1.65= x_1+ x_2$

4.2 Multiplicatively Homomorphic

To discuss the multiplicatively homomorphic of the rational, the new operation is defined in our approach, called fraction modular, expressing as "fmod" in short.

Definition 2: fmod is a binary operation, it is a fraction vs a large plus prime number to compute modular. fmod is yielded as fellow:

$$\text{fmod}(\frac{a}{b},p)= \frac{s\,\text{mod}(a,p)}{s\,\text{mod}(b,p)}$$

where a is a integer, b is a plus integer, p is a large plus prime number, and where smod() is similar modular operation. The security is not damaged where p is restricted a prime number greater-than zero.

Example:

$$\text{fmod}(\frac{17}{14},5)= \frac{s\,\text{mod}(17,5)}{s\,\text{mod}(14,5)}=\frac{2}{4}=0.5$$

Some properties of fmod are alike with properties common mod.

Theorem 1: $\text{fmod}(\frac{a_1}{b_2},p)\times\text{fmod}(\frac{a_2}{b_2},p)=\text{fmod}(\frac{a_1}{b_1}\times\frac{a_2}{b_2},p)$

Proof. According to the definition of the fmod:

$$\text{fmod}(\frac{a_1}{b_2},p)\times\text{fmod}(\frac{a_2}{b_2},p)$$

$$=\frac{s\,\text{mod}(a_1,p)}{s\,\text{mod}(b_1,p)}\times\frac{s\,\text{mod}(a_2,p)}{s\,\text{mod}(b_2,p)}$$

$$=\frac{s\,\text{mod}(a_1,p)\times s\,\text{mod}(a_2,p)}{s\,\text{mod}(b_1,p)\times s\,\text{mod}(b_2,p)}$$

$$=\frac{s\,\text{mod}(a_1\times a_2,p)}{s\,\text{mod}(b_1\times b_2,p)}=\text{fmod}(\frac{a_1}{b_1}\times\frac{a_2}{b_2},p)$$

As division is reverse operation of multiplication, the multiplicatively homomorphic of the rational is only discussed. The encryption and decryption algorithms are as follows:

Encryption:

① The algorithm of Multiplicatively homomorphic uses a large number, n, such that $n = p \times q$, where p and q are large security prime numbers. Let $Z_p = \{x \mid x \le p\}$ be the set of original plaintext messages, $Z_n = \{x \mid x < n\}$ be the set of ciphertext message.

② Given $x_1 \in Z_p$ and $x_2 \in Z_p$, to compute $x_1 \times x_2$, first of all calculating first of all x_1 and x_2 are expressed as fractions, namely $x1= \frac{a_1}{b_1}$, $x2=\frac{a_2}{b_2}$, where a_1 and a_2 are integers, b_1 and b_2 are plus integers.

③ For a_1, a_2, b_1 and b_2 , compute the encrypted value $y_{a1}= E_p(a_1)=\text{smod}((a_1+\text{sign}(a_1)\times\text{rand}()\times p),n)$, respectively, where rand() yields a random plus integer, and where sign(a_1) produces a plus or minus symbol like a_1.

④ Calculating $y_a= y_{a1}\times y_{a2}$ and $y_b= y_{b1}\times y_{b2}$, then counting $Y=\frac{y_a}{y_b}$, the result Y is encrypted automatically.

Decryption Given $Y=\frac{y_a}{y_b}$, use the key p to decrypt, $D_p(Y) = \text{fmod}(Y,p)= \frac{s\,\text{mod}(y_a,p)}{s\,\text{mod}(y_b,p)}$.

Example (Multiplication) Let p=101,q=71,n= p×q= 7171,x_1=1.4, x_2= -2.25.

According to the multiplicatively encryption algorithm:

x_1 and x_2 are expressed as fractions: $x_1=\frac{7}{5}$, $x_2= \frac{-9}{4}$.

a_1=7,b_1=5,a_2=-9 and b_2=4, compute the encrypted value ,respectively:

$y_{a1}=E(a_1)= \text{smod}((a_1+\text{sign}(a_1)\times\text{rand}()\times p),n)$
$=\text{smod}((7+123\times101), 7171)=5259$
$y_{b1}=E(b_1)= \text{smod}((b_1+\text{sign}(b_1)\times\text{rand}()\times p),n)$
$=\text{smod}((5+79\times101), 7171)=813$
$y_{a2}=E(a_2)= \text{smod}((a_2+\text{sign}(a_2)\times\text{rand}()\times p),n)$
$=\text{smod}((-9-222\times101), 7171)=-918$
$y_{b2}=E(b_2)= \text{smod}((b_2+\text{sign}(b_2)\times\text{rand}()\times p),n)$
$=\text{smod}((4+98\times101), 7171)=2731$

then calculating:
$y_a= y_{a1}\times y_{a2}=5259\times(-918)=-4827762$
$y_b= y_{b1}\times y_{b2}=813\times2731=2220303$
the result $Y=\frac{y_a}{y_b}=\frac{-4827762}{2220303}$

Decrypting Y yields,

$$\text{D(Y)=fmod(Y,p)}=\frac{s\,\text{mod}(y_a,p)}{s\,\text{mod}(y_b,p)}$$

$$=\frac{s\,\text{mod}(-4827762,101)}{s\,\text{mod}(2220303,101)}=\frac{-63}{20}=-3.15= x_1\times x_2$$

4.3 Analysis

The homomorphic encryption of the rational holds many properties. Due to using rand() in the encryption algorithms, there is one-to-many relationship, which implies that a single plaintext message, x, can have multiple ciphertext messages of $E(x)$ (i.e., although $E_1(x)\neq E_2(x)$, $D(E_1(x)) = D(E_2(x))$ is true for a plaintext message x).

Theorem 2: For all $x\in Z_p$, D(E(x))=x holds true.

Proof. Let y=E(x), a=x+sign(x)×rand()×p. Then it is true that y=smod(a,n)

Since n= p×q, the equation implies that
D(y)= smod(y,p)=smod(smod(a,n),p)
= smod(smod(x+sign(x)×rand()×p,n),p)=x

According to Domingo-Ferrer and Herrera-Joancomarti's discussion in Ref [5], the properties of security of the homomorphic encryption of the rational are as follows:

① **Ciphertext-Only Attack**. The cryptanalyst does not know p and gains a ciphertext $y \in Z_n$. However, p is needed to compute $a\ s\text{mod}\ p = x$. But, if the cryptanalyst sees only ciphertext, then finding the secret p from the public n is as difficult as factoring n [5]. Therefore, with only ciphertext, finding the original value is difficult.

② **Known-Plaintext Attack.** If the cryptanalyst knows a plaintext-ciphertext pair (x, y), then the cryptanalyst can generate a set of t numbers, $A_i \in Q_p$ for $i = 1, \ldots, t$ such that $A_i = y\ s\text{mod}\ n$. Then, the cryptanalyst knows that $A_i = x \bmod p$ for each i, so that $p \mid (A_i - x)$. With high probability $p = \gcd^{t}_{i=1}(A_i - x)$.

③ **Integrity Attack.** Since all of the decryption is performed modulo p, any unencrypted number $x < p$ will be deciphered as itself. Therefore an adversary can replace any encrypted value with a chose value and claim it is encrypted.

5. CONCLUSIONS

The approach in this paper can be used in many useful applications including multi-party computation, electronic voting, and mobile cryptography. Further considerations must

be taken for the improvement of our approach as follows:

① The homomorphic encryption is a simple cryptosystem, and requires extra work to develop more sophisticated encryption schemes with complete security analysis.

② In order to gain more secure cryptosystem, it is necessary to combine the homomorphic encryption and other encryption methods (e.g. function composition).

REFERENCES

[1] Diffie W, Hellman M. "New Direction in Cryptography",*IEEE Trans*,1976,22(6):644-654.

[2] Xiang GuangLi,Chen XinMeng. "A Method of Homomorphic Encryption," *Wuhan University Journal of Natural Sciences*,Vol.11, No.1, Jan.2006.181-184

[3] Haber S. "Multi-Party Cryptographic Computation: Techniques and applications" [Ph D dissertation], New York,Computer Science Department, Columbia University,1998.

[4] Rivest R L, Adleman L, Dertouzos M L. "On Data Banks and Privacy Homomorphism" [M]. *Foundations of Secure Computation*[C]. New York: Academic Press, 1978. 169-179.

[5] Domingo-Ferrer J, Herrera-Joancomarti J. "A New Privacy Homomorphism and Applications" [J]. *Information Processing Letters*, 1996, 60 (5): 277-282.

[6] Brickell E, Yacobi Y. On Privacy Homomorphisms[A]. *Advances in Cryptology—EUROCRYPT '87[C]*, Berlin German, 1987.

[7] Sander T, Tschudin C. "On Software Protection via Function Hiding," *Information Hiding*, Portland, USA, 1998.

[8] Sander T, Tschudin C. "Protecting Mobile Agents Against Malicious Hosts" [A]. In G. Vigna, editor. *Mobile Agent Security[C]*. Springer-Verlag: Heidelberg, Germany, 1998.

[9] Sander T, Tschudin C. "Towards mobile cryptography" [A].In *Proceedings of the IEEE Symposium on Security and Privacy[C]*, Oakland, CA, IEEE Computer Society Press, 1998.

[10] Lee H, Alves-Foss J, Harrison S. "The Use of Encrypted Functions for Mobile Agent Security" [A]. *Proceedings of the 37th Hawaii International Conference on System Sciences* – 2004[C]. Hawaii, USA, 2004

Ping Zhu (1980-),female ,PhD candidate, research direction: parallel and distributed computing, information security.

Trust-based Access Control Model for Grid Applications *

Hanbing Yao[1], Yangjun Liu[1], wei Liu[1], Ruixuan Li [2]
[1]School of Computer Science and Technology, Wuhan University of Technology
[2]School of Computer Science and Technology, Huazhong University of Science and Technology
Wuhan 430063, Hubei, China
Email: yaohb@whut.edu.cn

ABSTRACT

Despite the recent advances in access control approaches applicable to grid computing, there remain issues that impede the development of effective access control for grid. Grid provides people the way to share large mount of distributed resources and services that belong to different local organizations. These resources execute tasks submitted by users, who are not in the resources' local domain and hence have no control over these resources. Conversely these users are not controlled by the resource owners. Access control in computational grids is typically provided by a combination of identity certificates and local accounts. This approach does not scale as the number of users and resources increase. Moreover, identity-based access control is not sufficient because users and resources may reside in different security domains and may not have pre-existing knowledge about one another. Trust mechanism is well-suited for grid computing because it allows participants to establish mutual trust based on attributes other than identity. This paper describes the models of access control based on trust degree of grid entities, and dynamically manages the access permission according to the trust values of the subject and object. The basic rules of the trust-based scheme are presented, and the strategies are given for different access services in grid applications.

Keywords: Trust, Access control, Grid Security

1. INTRODUCTION

As the grid transitions from a purely scientific community to a heterogeneous, commercial, open community, it enters an environment of mutual suspicion. Malicious users can damage the grid by stealing sensitive information, corrupting data, and exhausting grid resources by severely exceeding the allocated resources [1,2]. Grid users are concerned with the privacy, confidentiality and integrity of their data.

Access control is one of the important security services according to the definition of IS07498-2 Security Architecture Model. Some access control models have been researched and applied widely: discretionary access control (DAC) [3], mandatory access control (MAC) [3], and role-based access control (RBAC) [4]. Existing access control model well suited for the centralized and relatively static environment, where the subjects, objects and resources are relatively static, and the permission that is granted for a subject to access a object is relatively changeless. In these access control model, the subjects are client processes or users, and the objects are usually server resources. Traditional access control models are not obviously suitable for the collaborative systems whose entities vary dynamically [5], such as grid computing.

Access control in grid computing is typically provided by a combination of identity certificates and local accounts [6]. Publicly available access control policies specify which users have access to what resources. Users are generally required to pre-register with a service provider before requesting a service. This approach does not scale as the number of users and resources increase and user population becomes highly dynamic. Furthermore, users and resources may be from different security domains with no pre-existing knowledge about one another. Digital certificates help to address some of these issues, but they do not guarantee that resources or users can be trusted.

In grid computing, the members and resources are dynamical, and the members might join or exit the system at any moment, and might be on-line or off-line. Otherwise, there is no super member or central node that assigns the roles or permissions to other members in grid computing. So it is not suitable that the access control is taken by assigning roles. In traditional client/server architecture, the security of access depends on identity authentication or authorization of trusted party, where the central node or trusted party is needed to participate. But the central entity or trusted party is often absent in grid computing, and the security system of data share and collaborative computation more depends on distributed trust system.

With these issues in mind, we propose a dynamic trust metric and trust-based access control model in grid applications. The trust-based access control model handles security problem on the whole of related network and system application instead of single system. The trust value might be from the experience with the target entity or the recommendation of other entities, or other specialized learning mechanism. The trust values among entities are not static, and vary along with the change of the context, so the entity's trust degree should be updated periodically and the access permission of an entity will vary relatively. Meanwhile, the variety of resources and services will result in the difference of requirement of the entity's trust value.

This paper is organized in five sections. After the Introduction in Section I, Section II describes related work about grid security. Section III explains our approach, proposes a flexible mathematical model for trust computation. Section IV describes trust-based access model. Section V concludes the paper and suggests future directions for improvement.

2. RELATED WORK ABOUT GRID SECURITY

In order to archive security in grid, some technologies have been used to build the security mechanism for grid. For example, in the Globus Toolkit (GT), a grid security infrastructure (GSI) has been established [6]. GSI defines a common credential format based on X.509 identity certificates

* This work was partially supported by National Natural Science Foundation of China under Grant 60403027, National Key Technologies R&D Program of China under Grant 2002BA103A04, and R&D Program of Hubei Provincial Department of Education under grant 2003A011.

and a common protocol based on transport layer security (TLS, SSL). Gateways are used to translate security policies between the common GSI infrastructure and local site mechanisms [7]. GSI supports many secure techniques, such as, single-sign, credentials, the collaboration between local secure strategy and secure strategy of whole system etc. GSI mainly points to secure the transport layer and application layer in network, and emphasize on synthesizing present popularly secure techniques to grids environment. The grid security can be provided as security services. Security messages and secured messages can be transported, understood, and manipulated by standard Web services tools and software. This mechanism is a good choice because the web service technology has been well established in the network-computing environment.

Although these secure techniques applied to grids are developing more and more mature, when they are applied to grid, there are many kinds of restrictions more or less [7,8]. For example, systems usually require the resources in different management domains can be trusted by each other, users must be all legal, applications are totally harmless, etc. These restrictions deeply frustrate the scale of grids, users and applications. Similarly, they may increase the cost of grid in running itself and implementing services, frustrate the development and applying into factual applications. At first, while actual computational grids can span several management domains, and in these domains, the very high trust relationship must be supported in each other. Computational resources in different domains usually should be shared for supporting powerful computing, while this kind of resources sharing may lead to illegal users acquire much higher secure level to access to the resources that they have no rights to access to. Under this condition, the security of resources is not assured, and even more the whole security of grid may be threatened. Secondly, if illegal users run Trojan horse in the environment of computational grid, certain resources in it may be destroyed and all information in it will disappear forever.

Applying trust to grid computing is a relatively new area of research. For example, Azzedin and Maheswaran define the notion of trust as consisting of identity trust and behavior trust [9-11]. They separate the “Grid domain” into a “Client domain” and a “resource domain”, and the way they calculate trust is limited in terms of computational scalability, because they try to consider all domains in the network; as the number of domains grows, the computational overhead grows as well.

Hwang et al. [12] and Sobolewski [13] try to build trust and security models for Grid environments, using trust metrics based on e-business criteria. Alunkal et al. [14] propose to build an infrastructure called “Grid Eigentrust” using a hierarchical model in which entities are connected to institutions which then form a VO. They conclude with the realization of a “Reputation Service”, however, without providing mechanisms that automatically can update trust values. Papalilo and Freisleben [15] has proposed a Bayesian based Trust model for Grid but the suggested metrics cover only limited trust aspects in practical Grid. TieYan et al. [16] consider trust only to improve the Grid Security Infrastructure (GSI) to achieve additional authentication means between Grid users and Grid services. Ching et al. [17] use the concepts of the subjective logic in the context of Grid computing using trust relationships to enhance the Grid security. Hui et al. [18] use the notion of “mission-aware” trust model, which take into account the cost of performing allocated tasks.

In the next Section, we will describe a trust model and trust computation using mathematic definition. The model supports security management in grid applications.

3. TRUST MECHANISM OF GRIDS

In grid system, all logged users can use grid resources through executing applications. While the fact is that users, resources and applications will not be reliable and beneficial for each other and so the security of grid becomes much more complicated. Some users passing authentications may illegally use grid resources out of their access rights, or acquire other users important data, some users pretend to share resources, in fact, their aim is to wreck grid resources and amend the result of applications, etc. From the above conditions, it is easy to see that security problems have already involved into every grid entity, including users, applications, computational resources and even network. Not only every entity has to face all kinds of insecure threatens, collaborating and sharing among these entities also involve many security problems. Nowadays, the secure problems in grids mainly include users security, computational resources security and applications security, and collaborative security among them etc.

As a result, study on the secure problems is the base to design security infrastructure for grid. Trust model is the effective way to implement the relationship among users, resources and applications.

3.1 Definition of Trust and Reputation

In the following defines, EX and EY represent the two entities, t is the time, and c is the context [9,10]. The notion of trust is a complex subject relating to a firm belief in attributes such as reliability, honesty, and competence of the trusted entity. There is a lack of consensus in the literature on the definition of trust and on what constitutes trust management.

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity’s behavior and applies only within a specific context at a given time.

Trust Level (TL) is built on past experiences and given for a specific context. That is, the firm belief is a dynamic value and spans over a set of values ranging from very trustworthy to very untrustworthy.

For example, entity Ey might trust entity Ex to use its storage resources but not to execute programs using these resources. The TL is specified within a given time because the TL today between two entities is not necessarily the same TL a year ago. For simplicity, we assume the trusts are divided into 6 levels (see Table1).

Table 1. Definition of trust level

Trust Level	Description
1	Very low trust level
2	Low trust level
3	Medium trust level
4	High trust level
5	Very high trust level
6	Extremely high trust level

Direct Trust is remarked as $\Delta(Ex, Ey, t, c)$ which represents the direct relationship of two entities in special time and

context.

Reputation is an expectation of entity's behavior based on other entities' observations or information about the entity's past behavior within a specific context of a given time. The reputation is remarked as $\Omega(Ex, Ey, t, c)$.

In computing trust and reputation, time factor have to be considered. For example, if Ex trusts Ey at level p based on past experience five years ago, the trust level today is very likely to be lower unless they have interacted since then. Similar time-based decay also applies for reputation.

Decay function is remarked as $\gamma(t - t_{tr}, c)$, where c is the specific context for the trust relationship, t is the current time, and tr is the time of the last update or the last transaction between Ex and Ey. The time factor t as explained earlier is very critical because information well-received from an entity five years ago might be ill-received today based on the validity of the information as well as how trustworthy is the entity today.

3.2 Computing Trust and Reputation

Let Ex and Ey denote two entities. The trust relationship based on a specific context c at a given time t between the two entities, expressed as $\Gamma(Ex, Ey, t, c)$, is computed based on direct trust relationships for the context c at time t between Ex, and Ey, expressed as $\Delta(Ex, Ey, t, c)$, as well as the reputation of Ey for the context c at time t expressed as $\Omega(Ex, Ey, t, c)$. The weights given to direct and reputation relationships are α and β, respectively. Since the "trustworthiness" of Ey is based more on direct relationship with Ex rather than the reputation of Ey, as far as Ex is concerned, α weighs more than β.

$$\Gamma(Ex, Ey, t, c) = \alpha \times \Delta(Ex, Ey, t, c) + \beta \times \Omega(Ex, Ey, t, c)$$
$$\alpha + \beta = 1$$

Direct relationship is computed as the product of the trust level in the direct-trust table (DTT) and the decay function $\gamma(t - t_r, c)$. In computing direct trust, historic directs transaction should be considered in countering malicious entities regarding strategic altering behavior.

$$\Delta(Ex, Ey, t, c) = \sum_{i}^{n} \alpha_i DDT(Ex, Ey, c) * \gamma(t_i - t_{tr}, c)$$
$$\alpha_1 + \alpha_2 + ... + \alpha_n = 1, 0 \le \alpha_i \le 1$$

The reputation of Ey is computed as the average of the direct trust of all entities which had transactions with Ey.

$$\Omega(Ex, Ey, t, c) = \sum_{i}^{n} \beta_i \Delta(Ezi, Ey, t, c), Ezi \neq Ex$$
$$\beta_1 + \beta_2 + ... + \beta_n = 1, 0 \le \beta_i \le 1$$

Currently, we are developing a trust management architecture that can evolve and maintain the trust values based on the concepts explained above. The rest of this paper is concerned with using the trust values maintained by such a system to perform efficient access control.

4. TRUST-BASED ACCESS CONTROL MODEL

In traditional centralized or client/server access control system, the subject's identity needs to be authenticated and the access permission is authorized according to its identity or role, and the access control means the control to the subject. But in grid environment, access control means the control both to the subjects and to the objects, and an access operation requires that the subject or object has certain trust degree, or both the subject and the object have certain trust degree. The trust values among entities are not static, and vary along with the change of the context, so the entity's trust degree should be updated periodically and the access permission of an entity will vary relatively. Meanwhile, the variety of resources and services will result in the difference of requirement of the entity's trust value.

4.1 Terminology

Entity: Entities might be members of grid or its processes, procedures, tasks, resources.

Subject: Subjects are entities that can perform operation on other entity. Subject might be grid members or its processes, procedures, tasks or resources.

Object: Objects are the entities that are accessed by other entities. An object might be grid member or its resource.

Operation: Operation means subject's atomic action on object, such as read, edit, browse, execution, query, etc.

Permission: An entity with access permission is granted to perform an operation.

Trust Value: Trust value is assumed to distribute from 0 to 1. Here 1 denotes absolutely trustworthy, and 0 denotes untruth at all.

Subject Trust Threshold: The subject trust threshold is defined as the minimum trust value of a subject for obtaining operation permission. When an entity's trust value is less than the subject trust threshold for an operation, the entity will be rejected to perform the operation because its trust value is not enough.

Object Trust Threshold*:* The object trust threshold is defined as the minimum trust value of an object that its resource can be accessed. When an entity's trust value is less than the object trust threshold for an operation, other entities will not to perform the operation on it because its trust value is not enough.

Trust update Deadline*:* The trust update deadline is the useful-life of a trust value. An entity's trust value should be updated at the trust update deadline.

Context*:* The context is the factors which have influence on entity's trust and access control, such as the importance of the object's resource, the recommender's trust degree, the network bandwidth and trust update period, etc.

4.2 Formal Definition

Definition 1: Trust-based access control model is a tuple as follows:
E is the set of entities
S⊆E is the set of subjects
O⊆E is the set of objects
OP is the set of operation on object's resources
TV: E×OP→[0,1], An entity's trust value for performing a operation.

TT_S: O×OP→[0,1], A subject trust threshold for performing a operation on an object.

TT_O: S×OP→[0,1], The object trust threshold which a object should have when subject performs a operation on it.

F: S×O×OP→[0,1], Access authorization rule. In trust-based access control model, the map F: S×O×OP→[0,1] denotes mapping the subject's operation permission on the object to set {0, 1}. Here 1 denotes that the access is permitted and 0 denotes that the access is denied.

When a subject will perform an operation on an object, the access control system judges the trust degree of subject and object as well as the context information of object's resources, and then decides to map the access permission to 0 or 1.

Definition 2: Trust-based access control policy is as follows:

$$\forall s \in S, o \in O, op \in OP$$
$$F(s,o,op) = TV(s,op) \geq TT\_S(o,op)$$
$$\&\&TV(o,p) \geq TT\_o(s,op)$$

If the trust value of subjects for performing the operation on o is not less than the subject trust threshold of performing operation op on object o, and the trust value of object o is not less than the object trust threshold that subject s performs operation op, the access permission is mapped to 1 and the access is permitted; or else the access permission is mapped to 0 and the access is denied. In this paper, the result of logic operation is 1 or 0, here 1 denotes true and 0 denotes false.

4.3 Basic Access Control Rules

Rule 1: When a subject performs an operation on an object, the trust value of the subject should not be less than the subject trust threshold that is required by performing the operation on the object; and meanwhile, the trust value of the object should not be less than the object trust threshold that is required by the subject's performing access.

Rule 2: When an entity's trust value has been kept over a period of time, it should be refreshed, and the access Rule permission of the relative entity will change correspondingly. The outdated trust value cannot be used for access control.

Rule 3: Access control is of relativity of its entity's context.

The trust value of an entity in grid system is relative to some other entity and it depends on the system context because the entity is various, dynamic and has no centralized control. The trust value that a subject should own for accessing an object' resource is relative to the importance of the resources. For instance, the trust value required for accessing an important resource is relatively higher than for accessing an ordinary resource. The context has influences on the access control of a system in various aspects.

For example, there is need that a subject evaluates object's trust value and the object evaluates subject's trust value when the subject wishes to submit a task on the object. The subject wishes to execute the task on a robust and not vicious object node and the task will not be modified or deleted viciously, or failure of system will not occur. The object wishes that the subject is trustworthy and the task from subject does not include virus, Trojan horse and other vicious data. The access control policy for executing the task is as follows:

$$\forall s \in S, o \in O, op \in OP$$
$$F(s,o,op) = TV(s,op) \geq TT\_S(o,op)$$
$$\&\&TV(o,p) \geq TT\_o(s,op)$$

5. CONCLUSION AND FUTURE RESEARCH

In a large-scale wide-area system such grid, how to secure resources is the hotspot in the filed of resource management. One approach is to be conservative and implement techniques such as sandboxing, encryption, and other access control mechanisms on all elements of the Grid. However, the overhead caused by such a design may reduce the advantages of grid computing. Furthermore, the existing access control mechanisms are not suitable for the access control of grid applications. In this paper, a novel trust-based access control is presented for access control of grid applications and other collaborative system. Further researches include the combination of trusted-based access control and role-based access control, the security mechanism of the access authentication, and the access control of other complex collaborative system.

REFERENCES

[1] I. Foster and C. Kesselman (eds.), “The Grid: Blueprint for a New Computing Infrastructure”, Morgan Kaufmann, San Fransisco, CA, 1999.

[2] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the Grid: Enabling scalable virtual organizations," Int’l Journal on Supercomputer Applications, 2001.

[3] L. Snyder, "Formal models of capability-based protection systems". IEEE Transactions on Computers, Vol. 30, 1981, pp. 172-181.

[4] R. S. Sandhu, E. J. Coyne, and H. L. Feinstein, "Role-based access control models", IEEE Computer, Vol.29, 1996, pp.38- 47.

[5] H. Shen and P. Dewan, "Access control for collaborative environments", in Proc. ACM Conf on Computer-Supported Cooperative Work (CSCW92). ACM Press, 1992, pp. 51-58.

[6] I. Foster and C. Kesselman, G. Tsudik, et al, A security architecture for computational grids. Proceedins of the 5th ACM Conference on Computer and Communications Security, San Francisco, CA, USA, 1998, pp.83-92.

[7] V. Welch, F. Siebenlist, I. Foster and J. Bresnahan, "Security for Grid Services", Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing (HPDC'03), 2003.

[8] L. Ramakrishnan, “Securing Next-Generation Grids”, IT Professional, vol. 20 ,2004, pp. 34-39

[9] F. Azzedin and M. Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems", Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID02), 2002, pp. 1-6.

[10] F. Azzedin and M. Maheswaran, “Evolving and Managing Trust in Grid Computing Systems”, Proceedings of the 2002 IEEE Canadian Conference on Electrical & Computer Engineering, 2002, pp.1424-1429.

[11] F. Azzedin, M. Maheswaran, “Integrating Trust into Grid Resource Management Systems”, International Conference on Parallel Processing, Vancouver, B.C.,

Canada. The International Association for Computers and Communications. IEEE Computer Society Press 2002, pp 47–54.
[12] K. Hwang, S. Tanachaiwiwat, “Trust Models and NetShield Architecture for Securing Grid Computing”, Journal of Grid Computing 2003.
[13] S. Goel, M. Sobolewski, “Trust and Security in Enterprise Grid Computing Environment”, Proceedings of the IASTED International Conference on Communication, Network and Information Security, New York, USA 2003.
[14] B. Alunkal, I. Veljkovic, “Reputation-Based Grid Resource Selection”, Workshop on Adaptive Grid Middleware (AgridM), New Orleans, Louisiana, USA 2003.
[15] E. Papalilo and B. Freisleben, "Towards a Flexible Trust Model for Grid Environments", GSEM 2004, LNCS 3270 Springer-Verlag Berlin Heidelberg 2004, pp. 94–106.
[16] L. Tie-Yan, Z. HuaFei, and L. Kwok-Yan, “A Novel Two-Level Trust Model for Grid”, ICICS 2003, LNCS 2836 Springer-Verlag Berlin Heidelberg 2003,pp. 214–225.
[17] L. Ching, V. Vijay and W. Yan, “Enhancing Grid Security with Trust Management”, Proceedings of the 2004 IEEE International Conference on Services Computing (SCC’04).
[18] L. Hui, P. Qinke, S. Junyi, and H. Baosheng, “A mission-aware behavior trust model for grid computing systems”, Proceedings of the International Workshop on Grid and Cooperative computing 2002 (GCC2002), 2002, pp. 883-890.

Hanbing Yao is a lecturer of School of Computer Science and Technology, Wuhan University of Technology; He graduated from the Huazhong University of Science and Technology and acquired the degree of Doctor in 2006. His research interests are in distributed system security, network security, grid computing and peer-to-peer computing.

The optimal Design to PID Controller of the Digital Closed-loop Instrument

Hongli Liu, Changxi Li
Department of Control Science &Engineering
Huazhong University of Science and Technology
Wuhan,Hubei province,China
Email: james97@163.com, changxilee@yeah.net

ABSTRACT

Taking the electronic balance digital display instrument as example, this paper analyses the influence of the every part of the digital closed-loop instrument on the dynamical performance of system, and builds up the system mathematical model. According to the desire of the dynamical performance indices of the system, two types of PID controllers are designed based on ITAE (the product integration of time and the absolute error) index and genetic algorithm respectively. Then the mathematical model built up is simulated with MATLAB language. The simulation results are shown that the digital closed-loop instrument with PID controller based on genetic algorithm has many advantages such as no overshot, shorter settling time, and parameter tuning simpler than that of ITAE index algorithm, so it can be suitable for the real application.

Keywords: Genetic Algorithm, ITAE Index, Digital Closed-Loop Instrument, PID Controller

1. INTRODUCTION

For the general control system, it is necessary to solve the problem of detecting objects at first, namely feedback, that we can achieve the purpose of control. The closed-loop instrument is a small power servo-control system. In order to obtain the measurement results, control is very important. Modern Instruments often integrate measurement with control, such as transmitters with fieldbus, which not only complete the task of measuring, but also achieve functions of controllers.

Many measurement and control tasks are accomplished by Algorithms.To improve the level and efficiency of study and development, and promote measurement and control technology mutual penetration, the common technology methods about modeling, analysis, simulation and control algorithm in control theory could be applied to the research and development of the closed-loop instruments. Adopting the principle of automatic voltage compensation, the digital closed-loop instrument can automatically measure and display all types of electrical parameter. With thermocouple, hot resistance or other transmitter, it can display and record the various parameters, such as temperature, pressure, flow, level, composition and so on. As a result of using microprocessor, it integrates measurement, subtraction, data processing, display, system adjustment and control, so it has better performances and more functions. In the digital closed-loop instrument, it is a key to design the PID controller optimally.

Nowadays, there are many methods of PID controller parameters tuning, such as the traditional PID algorithm, algorithm based on ITAE index and genetic algorithm etc. The algorithm based on ITAE index can reduce ITAE performance index to modify the transient response of the system, but genetic algorithm is easy to tune the parameters of PID controller accurately, and improve stability and dynamic characteristics of instrument.

2. THE MATHEMATICS MODEL OF DIGITAL BALANCE DISPLAY INSTRUMENT

The digital balance display instrument is composed with microprocessor, power amplifier, AC servo motor, a photoelectric encoder, ADC and DAC. Fig.1 shows its principle block diagram. After analog to digital conversion, DC voltage signal (input signal) input to microprocessor which compare the acquisition signal with the instrument point state information that is feedback signal by the photoelectric encoder. Microprocessor determines whether the point is corresponding to the input position. if not, according to the system dynamic performance indices, microprocessor processes the voltage difference data, calculates the corresponding control law to control servo motor to be forward-running or reversal, leads the point to reach position according to the input data, until balances between voltage and position.

The digital balance display instrument uses two digit switch signal to control power amplifier, which output the positive or negative 50Hz AC signal with the fixed amplitude, or zero signal. Because the power amplifier is vulnerable to be disturbed by work frequency, we often use phase-sensitive power amplifier to improve its resisting interference ability. In general a low pass filter circuit is added after phase-sensitive power amplifier, then the high harmonic of output signal is filtered. There we select ND-D-J3 AC servo motor in the laboratory, which its rated excitation voltage is 110V, rated control voltage 15V, idling speed 1250r • min^{-1}, slowdown ratio 1:39, the time constant 0.018s. Select 500 lines incremental optical encoder as a feedback sensor.

Supposed the entire system open-loop gain is K which can be equivalent into the digital controller $G_c(s)$. Thus, the open-loop transfer function of the digital balance display instrument is

$$G(s) = \frac{G_c(s)}{s(s+10)(s+471)} \quad (1)$$

3. CONTROLLER DESIGN

The digital balance display instrument is a position servo control system with light load, which demands rapid response speed, little overshoot and steady state error. For obtaining the better dynamical performance, it is necessary to adopt the digital controller to regulate system with better robust ， PID controller is so suitable to many kinds of operating condition that be used widely. The optimizing design to the parameter of PID controller draws attention.

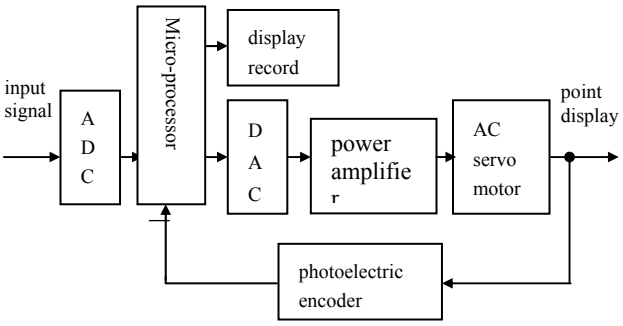


Fig.1. The structure principle diagram of digital balance display instrument

3.1 PID controller Design Based on ITAE Index

The design method to PID controller based on ITAE index can make ITAE performance index achieve the smallest, modify the step input or slopes input transient response of the system , meanwhile, reduce the influence of large initial error on the performance indices, but also stress the influence of in the recent response.

Supposed PID controller transfer function is

$$G_c(s) = \frac{K_2 s^2 + K_1 s + K_3}{s} \tag{2}$$

By using ITAE index, the optimal characteristic polynomial for system is

$$s^4 + 2.1\omega_n s^3 + 3.4\omega_n{}^2 s^2 + 2.7\omega_n{}^3 s + \omega_n{}^4 \tag{3}$$

According to ξ= 0.707 and settling time less than 40 ms, we can gain n=229.

Due to the existence of two zeros in the system, the system overshoot overload, so a pre-filter $G_p(s)$ is designed before the controller of the system to make the closed-loop transfer function the system standard form, and the system has the expect optimization. ITAE index

The standard form of closed-loop transfer function is:

$$T(s) = \frac{\omega_n{}^4}{s^4 + 2.1\omega_n s^3 + 3.4\omega_n{}^2 s^2 + 2.7\omega_n{}^3 s + \omega_n{}^4} \tag{4}$$

The transfer function of pre-filter is

$$G_p(s) = \frac{K_3}{K_2 s^2 + K_1 s + K_3} = \frac{1585}{s^2 + 84.87 s + 1585} \tag{5}$$

3.2 PID Controller Design Based on Genetic Algorithm

Parameter tuning method base on genetic algorithm is a high efficiency commitment method, which can seek global optimization solution without any initial information, and seek right parameter in the range.

The tuning processes of three parameters K_p, K_i and K_d base on genetic algorithm are follow:

(1) asceitain the scale of every parameter and the length of binary code, then encoder.
(2) produce at random initial population P(0)consisted of n individual.
(3) decode every individual of population into relevant parameter ,which is used to calculate the cost function value J and adaptive function value f, choose $f = \frac{1}{J}$.
(4) operate the population P（t）and produce the next generation population P（t+1）by copy ,crossover and mutation.
(5) repeat the processes (3) and (4)until obtaining the demand performance.

In order to obtain the satisfaction dynamic characteristics of the digital balance display Instrument, this paper adopts the absolute error time integral performance index as the minimum objective function of parameters selected. To prevent excessive control energy, the square item to control input is added to the objective function. In order to avoid overshoot, the objective function adopt the punishment factor, once overshoot is generated, overshot would be used as an optimal index. The follow equation is selected as the optimal performance index of PID tuning.

$$J = \int_0^\infty (w_1|e(t)| + w_2 u_2(t))\,dt + w_3 t_u$$
$$if \quad e(t) < 0,$$
$$J = \int_0^\infty (w_1|e(t)| + w_2 u_2(t) + w4|e(t)|)dt + w_3 t_u \tag{6}$$

In the equation (6), $e(t)$ is the system error, $u(t)$ is the output of the controller, t_u is the rise time, w_1, w_2, w_3, w_4 are weights, and $w_4 >> w_1$

4. THE STUDY OF MATLAB SIMULATION

Based on the above analysis, we use Matlab language to simulate analysis results. Fig.2 is the unit step response curve of display instrument for the PID control based on ITAE index. From the figure, we can see that PID controller without the pre-filter, the system's maximum overshoot is 70%, setting time is 45ms, the system overshoot is so overload that the

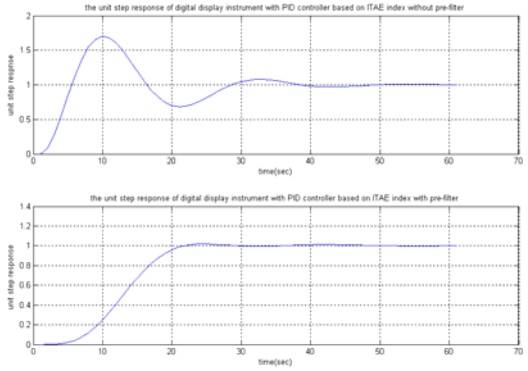


Fig.2. The step response of digital closed-loop instrument with PID controller based on ITAE index

controller can not work. Therefore, the pre-filter is designed before the closed-loop controller, then the system's overshoot is 2% and setting time is 20ms, the system dynamic performance is improved.

When the PID controller based on genetic algorithm is designed, the number of samples is 30, crossover probability P_c is 0. 9and mutation probability P_m is 0. 033, the range of parameter k_p is [0, 20], and the range of k_i, k_d are [0, 1]. Selected $w_1 = 0.999, w_2 = 0.001, w_3 = 2.0, w_4 = 100$, and simulate the system with real-number coding form. After 100

generations evolution, the optimized parameters k_p, k_i and k_d are 19.2421, 0.3324 and 0.7851 respectively, and the optimization value of performance index J equals 22.680. Fig.3 shows the optimizing process of cost function J, and fig.4 shows the step response of auto-balance digital display instrument based on genetic algorithm. The simulation results show that the overshot is zero, and the settling time is about 50ms, so the PID controller fulfils the demand of dynamical performance index.

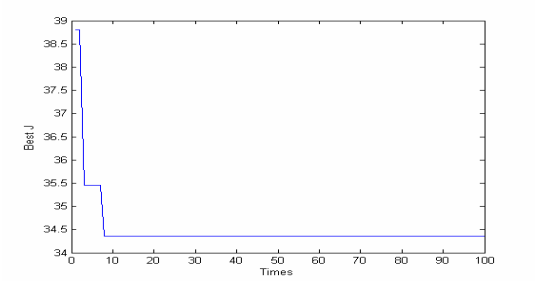


Fig.3. the optimization process of cost function J

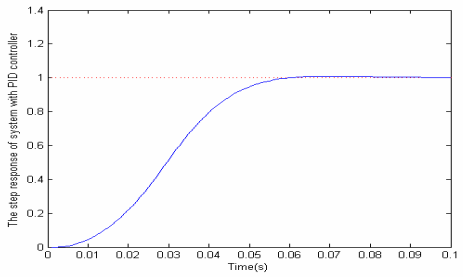


Fig.4. The unit step response of digital balance display instrument with PID controller based on genetic algorithm

5. CONCLUSIONS

Most of modern control instrument are that of digital closed-loop. In digital closed-loop instruments, micro-processor detects the state of instruments. If the state is imbalance, it send control signal to feedback mechanism according to a certain control law calculated, then make the instrument achieve a new balance. At this time, micro-processor r and the corresponding software is regarded as a digital regulator. From the control algorithms, the digital closed-loop instruments have the same role as the common digital regulator, and they all solve most of actual applications with the digital PID algorithm. Compared with the PID controller based on IATE index, the PID controller based on genetic algorithm needn't add any hardware structure, not only improve the PID tuning speed and accuracy, but also improve stability and dynamic characteristics.

REFERENCES

[1] Hongli Liu, Changxi Li, "Modeling and Simulation of the auto-balance digital display instrument," *Instrument technology and sensor* , 2004 vol257(7),13~14

[2] F.Xu, D.Li "Comparing and optimum seeking of PID tuning method based on ITAE index," *China Electrical Engineering Journal*, 2003.23(8). 206~210

[3] Q.Xie, H.Chen, "Optimization design of PID controller based on genetic algorithm," *Optics & Optoelectronic Technology* 2003.vol.1, no.3.pp 37~40.

[4] S. Liu, X. Peng, *The design of modern servo system,* Harbin Institute of Technology Press, Harbin, 2001.

[5] J.Liu, *The advanced PID control and MATLAB simulate*, Publishing House of Electronics Industry , Beijing, 2003

Research on Application of Dynamic Security Model in Electronic Commerce*

Xiaojun Tong, Minggen Cui, Jie Wang
Harbin Institute of Technology (WeiHai), School of Computer Science and Technology
WeiHai 264209, China
E-mail: tong_xiaojun@163.com, ziseshoulian2001@163.com

ABSTRACT

This paper focuses on issues related to deploying a data mining-based IDS (intrusion detection system) used in electronic commerce network, basing on the dynamic security model P^{2}DR. We present a modified Apriori algorithm with the concept of extreme item set, which represents an exponential number of association rules compactly. Experiment shows that this improved algorithm can reduce association rules effectively. Applying on IDS, it decreases the misinformation rate and the rate of fail to report an invasion behavior in intrusion detection system.

Keywords: Electronic commerce, Dynamic security model, Intrusion detective system, Data mining

1. INTRODUCTION

Researching on the electronic commerce network security has become a new study field recent years. Therefore dynamic security model P^{2}DR came into being. It can adapt to the dynamic multiform network environment, especially the protection, detection and response parts of network service layer in electronic commerce security framework. Intrusion detection system is the main technique means to realize the detection part in the security model P^{2}DR..

With the development of data mining technology, a lot of research works have been applied data mining in intrusion detection system. The project MADAM ID(A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems) of University Columbia in America used the associated rule and frequent rule to construct supererogatory forecast method[1,2]; Tsinghua University in China put forward a cooperating intrusion detection system (CoIDS) framework based on data mining. It used the Agent/Manager/UI three entity configuration and various data mining methods to found detection model [3].

This paper put forward a modified algorithm apriori_extreme based on algorithm Apriori. Experiment shows that it can reduce the number of associated rules in result set effectively. Applying on intrusion detection system, it can improve the dynamic security of electronic commerce network.

2. THE SECURITY TECHNIQUE FRAMEWORK IN ELECTRONIC COMMERCE

The key safety of the electronic commerce system is the safety that guarantee the business data and trades process. The inherent open character of Internet makes the electronic commerce system face various safe threats. In summary, the safety threats are listed below[4]:

The safety system framework of electronic commerce is a logic structure can guarantee the safety of electronic commerce data. It is constituted by five parts, such as figure 1shows [5].

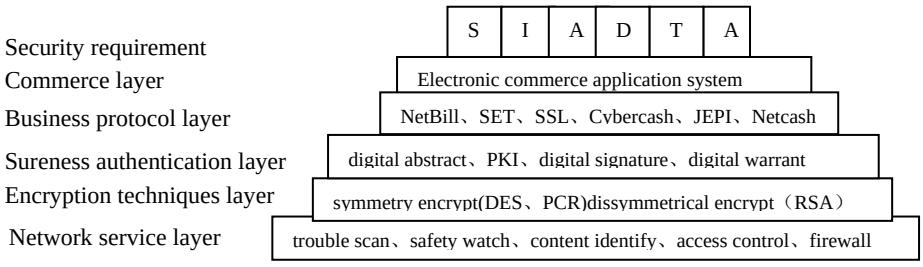


Fig.1. Electronic commerce safety system framework

PS: As seen above diagram, S represents security; I represents integrity; A represents anonymity; D represents anti-deny; T represents trustiness; A represents atomy.

3. DYNAMIC SECURITY MODEL P^{2}DR

Dynamic security model P^{2}DR (Policy Protection Detection Response) [6] integrate the safety policy, safety protect, and safety detect, response and resume together, which can guarantee the information safety effectively. See Figure2 shows the dynamic security .model P^{2}DR

Fig.2. Dynamic security model P^{2}DR

* The project is supported by 2006 stress natural science project fund of Shandong province in china(Project No. Z2006G01)
and by finance in Shandong Province science and technology plan project of china through the grant number 2006110

The P^2DR model is an advanced model. It must adjust in time with the diverse changing circumstance, and it also emphasizes on the cooperation among protection, detection and response system to ensure network security.

This model introduce into the time concept, which gives the operable description in how to realize the system safety and how to evaluate the safety state. There two typical mathematics formulas:

(1) Pt > (Dt + Rt)

(2) Et= Dt+ Rt, if Pt = 0

Among them: In order to establish various protection time that after protection, define Pt to delegate the time of hacker in attacking the system; The Dt delegate the duration from beginning invade the system to discover the intrusion; Rt delegate the duration from discovering intrusion to adjusts the system to normal sate; Et is the time that system exposure to hacker. Suppose the protection time Pt of the system to 0. Next we explain the formulas.

- Protection time Pt

In the P^2DR security model, when the hacker breaks into system, suppose that the intrusion detection system can detect and alarm the response part timely, so how strong the system is can be valued on the defense duration. Here the protection time is Pt, detection time is Dt, response time is Rt, if Pt > (Dt + Rt), then the network is safe.

Obviously the value of Pt is very difficult to estimate. Because one there is no much confidence in the protection system, the other is the means and level of the breaker is not all as the same. So based on this, from the absolute safety angle, we make Pt=0.

- Risk time Et

Now we have make Pt=0, that means the breaker needs no time to break the protection line. Because of the detection time and response time is (Dt + Rt), so for hacker they can be safe if they escape in (Dt + Rt) time. Now make Et = (Dt + Rt), we called Et is the network risk time, so Et reflect the size of network real risk.

The target is to eliminate the network risk, which means Et tends to 0. So it lies on network detection time and response time.

We can see from dissertate above, the detection and quick response are the ultimate approach to solve network security problem and to reduce the network risk. Unfortunately, many people want to install strong firewall or other protection implements to solve all the problems, we know it's a wrong way. First, we must analyze on the speed of system detection and response, make they are configured correctly, then via different measures to make Dt, Rt tend to 0, so the Et tends to 0.

4. RESEARCH ON DATA MINING ALGORITHM AND THE APPLICATION IN INTRUSION DETECTION SYSTEM

4.1 Apriori Algorithm and Related Research

The association rule is one of the main research modes of current data mining, which lay particular emphasis on connection relationship of different attribute in the record, and can reflect the interesting relationship of characteristic attribute, discover the internal and different characteristic attribute of each behavior records depend on a relation mutually. Algorithm Apriori[7]is the most typical and the most influential association data mining algorithm. Its basic thought is:

(1) Produce 1-frequency item set L_1, and then the 2-frenquncy item set L_2, till can extend the element number of frequency item set, and then stop.

(2) In the k-time circulation, the process create k-candidate item set C_K, then scan database using the minsupport then generate the k-frequency item set L_k.

(3) Using the frequency item set generate association rule. The basic principle of association generation is its confidence must bigger the supposed threshold. For an associating item set L, release its all null-empty subset R. When the confidence of $(L \Rightarrow R) \geq$ minconfidence, the rule $(L \Rightarrow R)$ can be seen as a association, then put out.

The above searching frequency item set algorithm takes up too much time, making the real-time of system could not reach a requirement; there are a great deal of association rule in the result set, so in this way come out many different optimized algorithm.

Moreover, some algorithm suggests the reduction the association rule number in result set. Document [8] for a survey of many interestingness measures proposed in the literature; a closely related work is[9], which proposed the concept of a closed frequent item set and used it to generate an exponentially smaller number of non-redundant association rules.

4.2 The Improved Apriori Algorithm

In this paper, we are not trying to reduce the number of association rules by choosing some of them or ignoring the others. Instead, we focus on the problem of compactly representing the association rules by a method of extreme item set, and the other association rules that cannot compact in extreme item set are handle alone. So in this way, we reduce the number of association rules in result set, make the data matching more easily in the data detective step, improve the algorithm efficiency.

4.2.1 Designing of the Extreme Item Set

Definition1.Let $s > 0$, $c \leq 100$ be the given support and confidence values. Define the item set G who is non-empty and number of element more than 2 is an extreme item set when X and Y are null-empty subsets belong to G, $X \cap Y = \phi$, $X \Rightarrow Y$ are all strong association rule. The element in extreme item set called the extreme item.

We can prove each such extreme item set can represent $3^n - 2^{n+1} + 1$ strong association rules tightly. Each of the element extreme items appears in the left side or it appears in the right side or it does not appear in either side. Thus the total number of possible rules for an extreme item set G of size n is bounded above by 3^n. Since neither the left side nor the right side of an association rule can be empty, we need to eliminate such association rules. The number of association rules where the left side is empty and the left side is any subset of the item set is 2^n. Similarly, the number of association rules where the right side is empty is also 2^n. Since the empty association rule is counted twice, so we get that a extreme item set seize of n can represent $3^n - 2^{n+1} + 1$ strong association rules. This expression is equivalent to the one in Proposition 1. Obviously, put forward the concept of extreme item set can cover exponential strong association rules successfully, improve the data matching in the detection step, then advance the whole system capability.

How find out the extreme item set, we set proposition as follows.

Proposition 1. Suppose $G=\{a_1, a_2, a_3,\ldots\ldots a_n\}$ is an item set whose element number more than 2. Let S_0 be the support of G, $S_1,S_2,\ldots\ldots S_n$ be the supports of the each item set

$\{a_1\},\{a_2\},\ldots\ldots\{a_n\}$ respectively. If the minimum support and confidence are s and c, then suppose Mn = $\min\{S_0,S_1,S_2,\ldots\ldots S_n\}$, Mx=$\max\{ S_0,S_1,S_2,\ldots\ldots S_n \}$. Then G is a extreme item set if （I）Mn ≥ s（II）(Mn / Mx) ≥ c .

Proof （I） Assume that（I）Mn ≥ s 和 （II）(Mn / Mx) ≥ c. G is an extreme item set if $X \Rightarrow Y$ is a strong association rule for any non-empty subsets of G. Let X and Y are any two non-empty subsets of G. We need to prove that support（X）≥ s，support（X∪ Y） ≥ s，[support（X∪ Y）/ support（X）] ≥ c. Given that support（X）≥ s, it follows that support（X）≥ s. Similarly, there is support（X∪ Y）≥ s. So comes that [support（X∪ Y）/ support（X）] ≥ Mn / support （X）≥ Mn / Mx ≥ c Since X,Y are arbitrary non-empty subsets of G, we have proved that G is a extreme item set.

（II） Assume that G is a extreme item set. We need to prove that （I）Mn ≥ s and（II）(Mn / Mx) ≥ c. Since Mx =$\max\{S_0,S_1,S_2,\ldots\ldots S_n\}$, let A = $\{a_k\}$ be a item and support （A）=support（$\{a_k\}$）= Mx. Let B be item set of all items from G except a_k. Clearly, A, B are two subsets of G. Since G is a extreme item set, A⇒ B is a strong association rule. Hence there are support（A）≥ s，support（A∪ B）≥ s, and [support（A∪ B）/ support（A）] ≥ c. Since support（A∪ B） = S_0 = Mn, it follows that Mn ≥ s, we have support（A） =support（$\{a_k\}$）= Mx, so have (Mn / Mx) ≥ c.

Using Proprsition1, we give an algorithm is_extremeset to judge whether an item set is the extreme item set.

It is clearly that this algorithm needs one pass over the database to obtain support for each subset of G, which needs to do it once only, so the algorithm complexity is O(N),where N equals to the number of transactions.

4.2.2 Improved Algorithm Apriori_Extreme.

(1) With the FP-tree, use the given transaction database to acquire an extreme item set G= $\{g_1,g_2, \ldots ,g_n\}$.
(2) At the initializing candidate step, not only combine each element in extreme item set to build up candidate C_2, but also must combine the non-extreme item in N.
(3) After discovery of k-frequency item set, the algorithm is the sub process who check whether there is any extreme item, if have, then add to G and meanwhile delete the sub item of this new comer in G.
(4) At this time if L_k becomes null, then stop the algorithm according to different instance.

Algorithm apriori_extreme
/*input the initial extreme item set G*/
input extremeset G = $\{g_1,g_2, \ldots ,g_n\}$
/*input the 1-frequency item set*/
input set of frequent item N = $\{f_1, f_2, \ldots , f_m\}$ where each $\{f_i\}$ is a frequent 1-itemset and $f_i \notin g_j$, for any g_j in G
input transaction database D, support s, confidence c
/*output all association rules*/
output set of association rules L $\Rightarrow$ R
/*output extreme item set G*/
output G
1. C_2 = {{u, v} | ($\exists 1 \le i, j \le k$ such that
$(u \in gi) \wedge (v \in gj) \wedge (i \neq j)) \vee (\exists 1 \le i \le m, 1 \le j \le k$
such that u= $fi \wedge v \in gj) \vee (\exists 1 \le i, j \le m$
such that $i \neq j \wedge u = fi \wedge v = fj$) } /find eligible C_2
2. Find support of all 2-itemsets in C_2 to determine L_2
/from C_2 get eligible L_2
3. add_to_extremeset (L_2, G) / add L_2 to G
4. k = 3; cease = 0;/setup the circulation condition
5. While cease = 0 do
6. C_k = gen_candidate_itemsets (G, N, k, L_{k_1})
/circulate generate C_k
7. Prune (C_k, G, N)
/pruning function generate new G
8. L_k = set of all candidates in C_k having support ≥ s
/from C_k get eligible L_k
9. If $L_k = \phi$; then cease = 1; endif
/meet the condition, exit from circulation
10. add_to_extremeset (L_k, G) / add L_k to G
11. end while
12. k++
13. result = $\cup L_k$ /result set unite all the frequency item sets

Algorithm add_to_extremeset
/realize the function of add new item to G
input L_k, G /input each frequency item set and G /from every circulation
1. for all itemsets l $\in L_k$ do
/ for all the item sets belong to the frequency item sets
2. if is_extremeset(l) then
3. G = G $\cup${l}
/add the subset of frequency item set to G
4. Remove all strict subsets of l from G
/delete all the subsets of the new subset
5. Lk = Lk - {l}
/delete the new add item set from Lk
6. endif
7. end for

The algorithm gen_candidate_itemsets is similar with Apriori which generate the candidate item set. The different is that the extreme item set size of k-1 can be seen as the k-1-frequency item set.

Next we explain this improve algorithm by giving an example. The table1 gives a transaction sample database; the minsuppot and minconfidence are 40% and 60% respectively.

Table 1. The transaction sample database

TID	Item set
1	A, B, C, D
2	B, C, E
3	A, B, C, E
4	B, D, E
5	A, B, C, D

Generate FP-tree of above database, Figure3 shows the FP-tree made from transaction sample database.

As the same reason, use the above FP-tree to construct the conditional FP-tree; making use of the modified FP-tree algorithm to generate the initial extreme item set

G={{A, B, C}}, so N={C, E}.
C_2={(AB,3),(AC,3),(AD,2),(AE,1),(BC,4),(BD,3),(BE,3), (CD,2),(CE,2),(DE,1)};
L_2 = {AB, AC, AD, BC, BD, BE, CD, CE}.

Use the algorithm is_extremeset to check L_2, and add the eligible item to G, so as follows

G = {{A, B, C},{A, D},{B, D}}

Notice that we use the pruning function in generating the new G, and cut off the sub item.

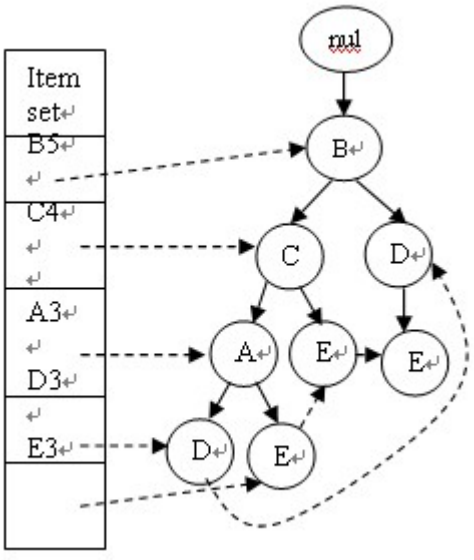


Fig.3. FP-tree made from transaction sample database

L_2 = { BE, CD, CE}.
C_3 ={(ABC,3),(ABD,2),(ACD,2),(BCD,2),(BCE,2)}
L_3 ={ABC, ABD, ACD, BCD, BCE}
Use algorithm is_extremeset again, then
G = {{A, B, C},{A, D},{B, D}}
C_4 = {(ABCD,2)}
L_4 = {ABCD}
G = {{A, B, C},{A, D},{B, D}}
$C_4 = \phi$ $L_5 = \phi$
cease = 1

After the whole algorithm, we get G = {{A, B, C},{A, D},{B, D}}, such extreme item represent 12,2,2 strong association rules respectively. In the example, we suppose the minsupport and minconfidence are 40% and 60% respectively, so at the end we use 3 extreme item sets represent 16 strong association rules in all. Thus we can directly see the optimized point, making the data mining in reducing the association rules contribute a lot.

5. EXPERIMENTS

In this paper, we use the DARPA99 network security audit dataset. There are five kind of attack: Denial of Service (DoS), Remote non-authorization access to local (R2L), non-root user exceed the privilege to root (U2R), spy and probing, data transmission attack.

In the experiment, we distill the characteristic attribute of HTTP protocol to cut off the message header info. The HTTP requirement follows with a lot of message header, which can be classified into three kinds: one is applied in requirement, one is applied in response, and the last describe the body. Some of the message header not only used in requirement but also in response, the message who describe body can show up in POST and all other response message. As table2 shows, the characteristic attribute distilled from HTTP visit record.

Table 2. HTTP protocol characteristic attribute

Name	ID	Time	SrcIP	DesIP	RequesMethod	RequestURL	ReCode	Sensitive info
The represent meaning	identifier	Time	The original IP address	The intent IP address	The method of requirement	The required URL	The returned code	The sensitive info in requirement or return

We divide the DARPA dataset into ideal size set, given the support equals to 0.5%,and confidence equals to 10%, Apriori algorithm generate 3856 association rules, apriori_extreme algorithm generate 216 extreme item sets, and the number of residuary association rules that cannot compressed in the extreme item set is 983, so obviously, it reduce 74.51%. From the experiment, we can conclude that apriori_extreme algorithm is better than Apriori algorithm, which compress the association rule effectively, advance the algorithm's efficiency.

In the intrusion aspect, about the misinformation rate and the rate of fail to report a invasion behavior in intrusion detective system, we given 1354 normal records include in the dataset, the intrusion data is 488 records, similarly use the support equals to 0.5% and confidence equals to 10%, we get the following data, there are two detection result of two algorithm, as table 3 shows the DARPA99 test data result.

Table 3. DARPA99 test data result

Algorithm	Normal data number	Invade data number	N_to_I	I_to_N	Misinformation rate	The rate of fail to report
Apriori	1125	717	513	350	27.9%	19%
apriori_extreme	1264	578	406	298	22%	16.2%

PS: Here N_to_I represents the number of normal data which is detected to be intrusion data, I_to_N represents the number of intrusion data which is detected to be normal data.

From above result we can see clearly that the apriori_extreme has a lower rate of the misinformation rate and the rate of fail to report an invasion behavior in intrusion detective system, than Apriori algorithm, proving this algorithm has advantage when applying to intrusion detection system, which can give more guarantee of the dynamic safety in electronic commerce network.

6. CONCLUSIONS

We put forward the concept of extreme item set and the modified algorithm apriori_extreme. Experiment shows that the extreme item set can cover exponential number of association rules compactly and improve the algorithm efficiency. Besides that the experiment proves the apriori_extreme has lowered by 5.9% rate in the misinformation rate and by 2.8% rate in the

rate of fail to report an invasion behavior in intrusion detection system. Therefore constructing the intrusion detection system based on this term, it can enhance the dynamic security in electronic commerce network.

REFERENCES

[1] Lee W, Stolfo S J, *Mok K W. A Data Mining Framework for Building Intrusion Detection Models*. *in Proceedings of the 1999 IEEE Symposium on Security and Privacy*,pp120-132,1999

[2] Lee W , Stolfo S J, Mok K W. *Data Mining Approaches for Intrusion Detection. In:Proceedings of the Seventh USENIX Security Symposium* (SECURITY '98), pp 120-132, 1998

[3] Duan Hai-xin,Wu Jian-ping: *Design and realize a kind of distribute type cooperation intrusion detection system, software journa*,Vol.9,pp1375-1379,Dec,2001

[4] Camp L,Harkavy M, Tygar J *D.Anonymous Atomic Transaction*,In *Proceedings of the 2"d USENIX Workshop on Electronic Commerce*, ppl23,1996

[5] Tygar F *D.Atomicity in Electronic Commerce*. *in Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing*,pp8-26,1996

[6] Yang Yi-xian, Niu Xin-xin:"the network safe theories and technique", people post publisher,pp182, 2003

[7] Rakesh Sgrawal, Ramakrishnan Srikant. *Fast Algorithm for Mining Association Rules*. Proceedings of 20th Int. Conf. *Very Large Data Bases (VLDB)*, Jorge B. Bocca, Matthias Jarke and Carlo Zaniolo, eds.Morgan Kaufmann Press,487-499, 1994

[8] R.J. Hilderman, H.J. Hamilton, *Knowledge discovery and interestingness measures: a survey, Tech*. Report CS-99-04, Dept. of Computer Science, Univ. of Regina, pp87-91, 1999:

[9] M.J. Zaki, *Generating non-redundant association rules, in Proc. 6th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining (KDD-2000)*, pp.34–43, 2000

Xiaojun Tong: A vice professor, birth 1963, reading Ph.D. at Harbin Institute of Technology. Research direction: chaos cryptography, information security.
Communicate address: Harbin Institute of Technology (Weihai) in school 20#506 room, Weihai, 264209, P.R. China
E-mail: tong_xiaojun@163.com

Minggen Cui Professor, Director of PhD candidate.

Petri Dish of Large Scale Worm Online Tracing *

Yang Xiang, Qiang Li
College of Computer Science and Technology, JiLin University
Changchun, JiLin 130012, China
Email: li_qiang@jlu.edu.cn

ABSTRACT

Breaking out of network worms brings a tremendous damage to the Internet. Launch the worm defense and response can improve network anti-strike capability. Tracing worm propagation path after its outbreak can reconstruct not only the earliest infected nodes but also the timing order of victims been infected. For the detection and defense of large scale Internet worm outbreaks, a convenient and safety experimental environment that capable of running real worm become an important work to observe large scale worm infection, intrusion and propagation, it can be a large scale worm testbed for forensic evidence. This paper presents a large-scale worm propagation experiments environment for tracing algorithm, which is an isolation environment that can run related experiments. To conform as much as really to the actual network, the experimental environment use virtual machine technology, simulate a large number of hosts and network equipments attend. According to the actual worm, this environment can trigger large-scale worm outbreaks within the controllable scope of human, observe propagation process of the worm, experiment detection and defense techniques, discover worm propagation characteristic such as scanning method and propagation process, real-time collect network traffic and propagation process, investigate network traffic, launch speculate algorithm for reconstructing out patient zero and propagation path of the worm. Then actual worm propagation process can be captured and compared with the results using tracing algorithm.

Keywords: Worm, Online Tracing, Petri Dish

1. INTRODUCTION

Worm outbreaks are security events that occur with relatively low frequency, but when they do occur, they can compromise thousand of hosts in short time, launch DDoS attacks, steal security information and destroy key data. So worm outbreak has terrible influence each time. Currently, research on worm detection and containment continuously improved, tracing the evolution of a worm outbreak (attacking path of worm) is an important research area[1,2,3], it not only reconstruct patient zero (i.e., the initial victim), but also the infection node list in evolution process. The reconstruction result has significance in restraining evolution of worm and forensic evidence.

Large scale network worm tracing research needs a reliable algorithm experimental environment. First, real time tracing algorithm needs to carry out theoretical analysis, and prove the correctness of tracing algorithm under some assumptions and prerequisite conditions. Second, different tracing model with different parameters in the algorithm are established. But theoretical deduce can not reflect the real execution of algorithm. Many researchers use some network simulation platform like ns2 [4] or parallel-ns2 to establish the tracing simulation testing environment, simulate running thousands of nodes in different network topology and bandwidth. But simulation is more applicable to modeling, not real worm spread. Simulation process is too idealistic, not a true reflect of the operating system and demand high performance experimental host. Using physical host for large-scale network worm tracing experiment is also unfeasible. First thousands of physical hosts can not be guaranteed. Second, because of worms destructive, the large number of physical host unable to quickly reuse, management and configuration workload is huge.

In recent years, virtual machine technology's development promoted its application in the field of network security research. Researchers have begun network worm detection and defense experiments using virtual machine technology [5, 6, 7]. One physical host can run a number of virtual machine installed real operating system, and connected to the network. External visitors perceived no internal differences except for a little performance odds. So they can use the virtual machine technology to establish a high realistically, control flexibility, encapsulate and reusable virtual experimental environment. After optimize virtual machine and the installed operating system, the performance requirements of physical host can be reduced. Optimal use of virtual machine technology can simulate thousands of virtual operating system nodes in nearly dozens of physical host, more clearly discover propagation process of network worm in the operating system and network, further observe invaders motivation, tools and methods.

This paper presents a large scale worm propagation experiments environment for a tracing algorithm, which is an isolation environment that can progress related experiments. To conform as much as possible to the actual network, the experimental environment use virtual machine technology, simulate a large number of hosts and network equipments attend. According to the actual worm, this environment can trigger large scale worm outbreaks within the controllable scope of human, observe propagation process of the worm, experiment detection and defense techniques, discover worm propagation characteristic such as scanning method and propagation process, real-time collect network flows and propagation process, investigate network traffic, launch speculate algorithm to rooting out patient zero and propagation paths of the worm. Then capture real worm propagation process, and compare with the results using tracing algorithm.

This paper follows as: Part 2 introduces composition of the Petri Dish; Part 3 shows a main functional design of Petri Dish; Part 4 gives a specific example of experiment; Part 5 is concluded.

2. PETRI DISH

To establish a Petri Dish for large-scale worm tracing has the following main objectives: a), worm experiments can be fully controlled within the scope of human, the start-up and shut down of experimental environment dominated by the

* Supported by NSFC(90204014) and Seed Fund of JiLin University.
Corresponding author: Qiang Li, li_qiang@jlu.edu.cn

experimenter, b), the experimental environment is independent and self networking, communications with the outside world under surveillance, c), experimental process and results can fully be observed, true infection and algorithm results can be compared, d), the experimental environment can be reused, minimized the cost of maintaining.

Fig. 1 shows the diagram of the large-scale worm online tracing Petri Dish. The whole environment is composed by multiple physical hosts and switch components. Physical hosts connect each other form a LAN through switches.

UML[8] is a lightweight virtual machine system on Linux. It can run numerous instances on physical host, with the various versions of Linux operation systems. It can customize operation system of the virtual machine according to the requirement; only need install the necessary system software and system services. Therefore it has a higher performance and occupy fewer resources of the physical host.

Each host installs a UML system in the experimental environment, running advance customized client operating system image, serve as various experimental roles according to the pre-configuration. After environment launched, several virtual machines in a physical host form a virtual local network (VN), and connected via UML virtual switch. Each physical host, as a gateway of its own local network, connects other VNs on other host. Extending like this, a basic multi-VN experimental environment can be setup.

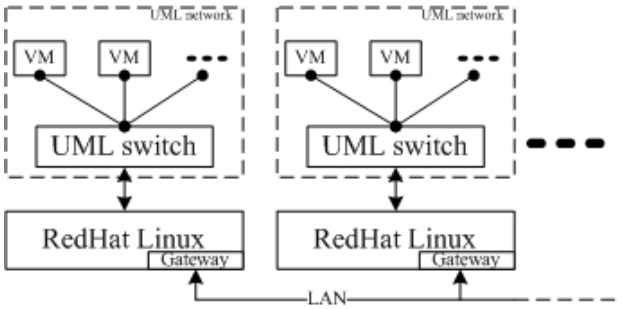


Fig.1. Diagram of the large-scale worm online tracking Petri Dish

In this virtual environment, many virtual clients in a physical host have system security security holes, and they can be infected by worms. In order to control propagation process of the worm, the Petri Dish has some functional modules showing in Fig. 2. Virtual clients in the Petri Dish is using real operating system, and running some services with security holes. Main functions are as follows:

a) virtual environment startup and shutdown
Launch related startup script after physical host LAN is ready, and then start all virtual machines in every physical host. Hosts and virtual clients have to execute initialization script, configure network connections and some other issues.
b) Worm launch
A random virtual client is selected, and executes worm startup script. The script first infected the chosen virtual machine, and then begins to propagate.
c) Infections collect
During the worm propagation, each virtual machine is monitoring its own change of infection characteristic according to the pre-configurations. Once infected, the infection details will be recorded in the host.
d) Network flows collect
After virtual environment startup, every host has the responsibility of monitoring communications between its VN and other VNs of other hosts. Based on predetermined monitoring rules, hosts capture data and transfer to the unified host running tracing algorithm.

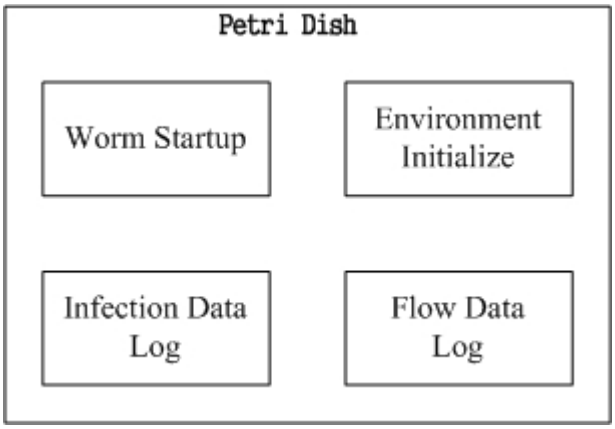


Fig.2. functional modules of Petri Dish

3. DESIGN

According to the propagation characteristics of the worm, the Petri Dish accomplish its missions mainly depend on network traffic collection model and various scripts.

3.1 Virtual Client System

Virtual client system uses Linux version with security holes. To facilitate the maintenance, all the virtual systems adopt a unified system image file, so the operating system software installed exactly the same. Each virtual client is running different initialization script based on its own id, and completing their respective functions. Using the COW(Copy On Write) technology of UML, all virtual machines only use one unify image file when startup virtual operation system, and create their own differences file to storing data. In this way can avoid each virtual client use a separated virtual image, improve the system efficiency, and reduce the storage space required. When launching the virtual environment, experimenter can specify the number of running virtual machines and their operating roles. For example, the virtual client startup command is like this:

../linux ubd0=cow$1,../root_fs umid=uml$1 eth0=daemon,,unix,/tmp/umlsw con=xterm con1=null con2=null &

3.2 Host Network Configuration

HOST network configurations separated into two parts. First interconnect all VNs in physical hosts. Then physical hosts should connect their VN to the LAN. Implementation steps are as follows:

a) Fetch network addresses configuration file, startup virtual switch (uml_switch) to interconnect all virtual clients on a physical host. Then configure address information of virtual switches.
b) Set up packets transmits and ARP resolve of every physical host, ensure that host can communicate with its virtual clients.
c) Use route command to set up routing tables between different VNs, ensure that virtual clients on different hosts can communication each other.

The main commands of configuration script are as follows:
uml_switch -hub -tap tap0 -unix /tmp/umlsw -daemon
ifconfig tap0 192.168.$NET.1 netmask 255.255.255.0 up
echo 1 > /proc/sys/net/ipv4/ip_forward
route add -host 192.168.$NET.$i dev tap0
echo 1 > /proc/sys/net/ipv4/conf/tap0/proxy_arp
arp -Ds 192.168.$NET.$i eth0 pub

3.3 Virtual Client Network Configuration

a) Launch virtual client; fetch its id according to the corresponding startup command.
b) Set up its VN address according to the fetched id.
c) Set the type of startup service.

3.4 Background Flows and Data Collection

Starting up HTTP service and running lynx command in the active virtual machine, and generating background flows according to the predetermined time cycle. Every host running tcpdump, collect network flows according to some rules and transmit to the designated host.

4. EXPERIMENT

Using UML virtual machine technology, we establish an experimental environment include 200 virtual nodes base on 7 PCs. Virtual clients running Redhat Linux 6.1 operation system with BIND security holes. Physical hosts running Redhat Linux 9.0 operating system. Several virtual clients in a physical host form a VN, virtual clients in different host communicate with each other using gateway in every physical host. This environment can be independently reused. Nodes and network topology can be flexibility configured. Experimenters enable to collect network data and infections for analysis after the outbreak of worm.

Manually launch a worm propagation break source in one of the four LANs, startup Lion worm attack [9], then running tracing algorithm to analyze the final result and true infections. The continuous real time collection network flows include not only worm flows, but also pre-installed normal background flows.

The collected flows are shown as the following example:
15:13:09.939800 192.168.0.154.1036 > 192.168.0.150.domain
15:13:09.942412 192.168.0.150.domain > 192.168.0.154.1036
15:13:09.945855 192.168.0.154.1036 > 192.168.0.150.domain
15:13:10.000830 192.168.0.150.domain > 192.168.0.154.1036

Infection report is shown as the following example:
From 192.168.0.154 Fri Jan 19 02:13:17 EST 2007 To 192.168.0.150
From 192.168.1.107 Fri Jan 19 02:15:07 EST 2007 To 192.168.0.153
From 192.168.0.150 Fri Jan 19 02:15:48 EST 2007 To 192.168.0.145

Fig.3 shows the worm infected tree analyzed by the tracking algorithm:

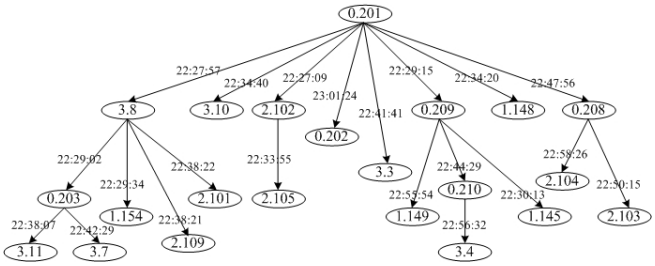


Fig.3. worm infection tree

5. CONCLUSIONS

Worm experiment can be done in a high reality and flexibility using virtual machine technology. Experiment is non-proliferation, not destructive, and can effective use resources simulate thousands of nodes. Worm destruction process can be seen more realistically.

Compare with other worm experimental environments [5, 6, 7]. The Petri Dish has the following characteristics: a), real-time collect all the network flows including normal background flows and worm propagation flows in the experimental environment, b), tracking algorithm can be deployed, online display tracking result, c), can be configured individually for each node and network topology, d), recur the worm detection, intrusion and propagation process.

REFERENCES

[1] D. M. Kienzle and M. C. Elder. “Recent worms: a survey and trends.” In WORM ‘03: *Proceedings of the 2003 ACM workshop on Rapid Malcode*, pages 1–10, New York, NY, USA, 2003. ACM Press.
[2] Abu Rajab, M., Monrose, F., and Terzis, “A. Worm evolution tracking via timing analysis.” In *Proceedings of the 2005 ACM Workshop on Rapid Malcode* (Fairfax, VA, USA, November 11 - 11, 2005). WORM '05. ACM Press, New York, NY, 52-59.
[3] Yinglian Xie, Vyas Sckar, David A.Maltz,Michael K. Reiter, and Hui Zhang. “Worm Origin Identification Using Random Moonwalks.” In *Proceedings of IEEE Symposium on Security and Privacy*, pages 242–256, May 2005.
[4] The Network Simulator-2, http://www.isi.edu/nsnam/ns/, 2004.
[5] X. Jiang, D. Xu, H. J. Wang, and E. H. Spafford, "Virtual Playgrounds for Worm Behavior Investigation", *Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection* (RAID 2005), Seattle, WA, September 2005.
[6] Michael Vrable, Justin Ma, Jay chen, David Moore, Erik Vandekieft, Alex C. Snoeren, Geoffrey M. Voelker and Stefan Savage, Scalability, Fidelity and Containment in the Potemkin Virtual Honeyfarm, *Proceedings of the ACM Symposium on Operating System Principles* (SOSP), Brighton, UK, October 2005.
[7] Michael Vrable, Justin MaSamuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, Jacob R. Lorch, "SubVirt: Implementing malware with virtual machines", *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, May 2006.
[8] J. Dike. User Mode Linux. http://user-mode-linux.sourceforge.net.
[9] Linux Lion Worms. http://www.whitehats.com/library/worms/lion/, 2001.

Specifying the Needham-Schroeder Symmetric-Key Cryptographic Protocol in the Ambient Calculus

Minglong Qi, Qiping Guo, Luo Zhong
School of Computer Science & Technology, Wuhan University of Technology,
Ma Fang Shan Campus, 430070 Wuhan China
E-mail: **mlki01@sohu.com**

ABSTRACT

In this article, we have used a variant of the Mobile Ambient, called Extension Boxed Ambient or NBA, to formally specify the famous Needham-Schroeder symmetric-key cryptographic protocol. The specification has been proven to be well formed, and capture the essential aspects of the protocol. The paper has demonstrated that, instead of the pure Mobile Ambient inheriting non-determinism and interference of movement of ambients, the NBA is a tool suitable for specification of protocols.

Keywords: Mobile Ambient, Ambient Calculi, NBA, Needham-Schroeder Symmetric-key Protocol

1. INTRODUCTION

Traditionally, cryptographic protocols have been designed and verified using informal and intuitive techniques. It is true that, humane creative activities are often formulated and set in form by means of informal and intuitive methods. But these lasts may often lead to flaws or errors, namely in the design and verification of transport or cryptographic protocols. For example, a flaw in the famous Needham-Schroeder symmetric-key protocol [1] has been found in a work presented in [2]. Consequently, formal specification and verification in the protocol design become an absolute necessity for the validation and security of these lasts. Recently, a number of formal techniques, either algebraic or logic, have been developed for this purpose. For example, a process algebra called SPI calculus [3] has been specially conceived for the specification and verification of secure cryptographic protocols, and a successful case study of which for specifying and verifying the Needham-Schroeder protocol can be referred in [4]. Of course, classical process algebras such as CSP [5] are always valid in this kind of situation [6]. Cryptographic or transport protocols present some common features: distributed locations in network, mobility of data and codes, and concurrency and parallelism of processes, etc. Cardelli and Gordon [7] have invented a powerful process calculus called Mobile Ambient (MA). It is powerful because it is very suitable for modeling distributed, mobile and parallel behaviors. In addition, some principal variants of MA such as Boxed Ambient [8], Extension of Boxed Ambient (NBA)[9], Chanel Boxed Ambient [10], Secure MA [11], etc, have been born for remedying a leak of security and communication mechanism of MA.

In this paper, we are aiming at formally specifying the Needham-Schroeder symmetric-key protocol using a variant of MA: Extension of Boxed Ambient (NBA)[9]. The article is structured as fellows: in section 2, we briefly introduces the Controlled Boxed Ambient; in section 3, we informally present the Needham-Schroeder protocol; in section 4, we formulate formally the results of this article; in section 5, we describe shortly the related works and in section 6, we conclude our work.

2. THE EXTENSION BOXED AMBIENT (NBA)

The calculus of Mobile Ambients [7] (MA) introduced an important notion that is ambient. An ambient is a named location that may contain processes and children ambients, and that can move as a unit inside or outside other ambients. Processes within an ambient may cause their surrounding ambient to move, and may communicate with their parent ambient or sibling ambients.

In MA, there are two capabilities that control ambient movements: ***in*** and ***out***. The process with ***in*** capacity can make its surrounding ambient to move inside a sibling ambient, while the one with the ***out*** capacity can make its surrounding ambient to go out of the parent ambient. Another important capability is ***open***, which permit to dissolve an ambient. These three capabilities are characterized by three correspondent reductive equations following:

$$m[in\ n.P \mid Q] \mid n[R] \rightarrow n[R \mid m[P \mid Q]] \quad (2.1)$$

$$m[P \mid n[out\ m.Q \mid R]] \rightarrow n[Q \mid R] \mid m[P] \quad (2.2)$$

$$m[P \mid n[Q] \mid open\ n.R] \rightarrow m[P \mid Q \mid R] \quad (2.3)$$

where ***m***, ***n*** are the names of ambients, ***P***, ***Q*** and ***R*** are of processes, ***in n.P***, ***out m.Q***, and ***open n.R*** are respectively the processes headed by the ***in***, ***out***, and ***open*** capabilities, while square brackets delimit ambient' contents. For explaining the communicative mechanism in the MA, please read the process expressed in the equation (2.3):

$$a[\,p[out\ a.in\ b. < M >]] \mid b[open\ p.(x).Q] \quad (2.4)$$

The process (2.4) models the movement of a packet ***p*** in form of an ambient, which contains a message ***M*** to output, from location ***a*** to location ***b***. The ambient ***p*** contains a single process ***out a.in b.<M>***, that allow ***p*** to go out of the ambient ***a***, enter inside the ambient ***b***, and finally drop the message ***M*** in the ether of the ambient ***b*** with the condition that the ***b*** will be dissolved. The ambient ***b*** contains a single process ***open p.(x).Q***, that at first open the ambient ***p***, and wait for reading a message by the sub process ***(x)*** from the ether of its parent ambient. Once the ambient ***p*** is opened, its process drops the message ***M*** in the ether of the ambient ***b***, and at the moment the process ***(x).Q*** can read the message ***M*** and continue to beehive as ***Q*** with all occurrences of ***x*** in ***Q*** substituted by ***M***. Finally, the equation (2.4) is reduced to $a[] \mid b[Q\{x := M\}]$.

As we said, the MA is very powerful because it captures all essential aspects of distributed systems: distributed locations, agent mobility, and concurrency, etc. But in the same time, it has posed some new hard problems. In [12], the authors have revealed some so-called grave interference, that is, situations where the inherent non determinism of movement goes wild. For illustrating this kind of situations, we just consider a case expressed in the equation (2.5):

$$k[n[in\ m.P \mid out\ k.R] \mid m[Q]] \quad (2.5)$$

Two processes ***in m.P*** and ***out k.R*** of the ambient ***n*** are paralleled to be competitive, leading the behavior of the enclosing ambient to a desperate non determinism. Another source of problems resides at the capacity ***open*** that may cause some grave impasses due to security accounts in eventually real implementation of the calculus.

The extension of Boxed Ambient (NBA), adopts the co-capacities for eliminating the non-determinism in MA, and a communicative mechanism crossing the boundaries between parent and children ambients. In order to enter into a sibling ambient, not only the concerned ambient should own an ***in*** capability, but also the target ambient should own a correspondent co-capability, and in addition, two sides should agree on to a common password. The equation, with the in capability of two formal parameters, becomes as (2.6):

$$n[enter < m,k > .P1 \mid P2] \mid m[\overline{enter}(x,k).Q1 \mid Q2] \rightarrow$$
$$m[n[P1 \mid P2] \mid Q1\{x := n\} \mid Q2] \qquad (2.6)$$

Notice that the capacity ***in*** is substituted by the capability ***enter***, and the variable ***x*** refers to the name of the ambient incoming, that is very useful in the transfer of data between several ambients. With the co-capabilities, we can now resolve the problem of non determinism expressed in equation (2.5) by the formalism of NBA, shown in equation (2.7):

$$k[n[enter < m,k1 > .P \mid exit < k,k2 >] \mid m[\overline{enter}(x,k1).Q] \qquad (2.7.1)$$
$$k[n[enter < m,k1 > .P \mid exit < k,k2 >] \mid m[Q] \mid \overline{exit}(x,k2) \qquad (2.7.2)$$

As for the communicative mechanism, the NBA permits ambients to communicate through the boundaries of the parent and the children ambients. This is resumed in the next equations:

$$(LOCAL) \qquad (x).P \mid < M > .Q \rightarrow P\{x := M\} \mid Q$$
$$(INPUT\ n) \qquad (x)^n.P \mid n[< M >^{\uparrow}.Q \mid R] \rightarrow P\{x := M\} \mid n[Q \mid R]$$
$$(OUTPUT\ n) \qquad < M >^n.P \mid n[(x)^{\uparrow}.Q \mid R] \rightarrow P \mid n[Q\{x := M\} \mid R]$$

In the above equations, a process as $< M >^{\uparrow}$ is a upward output, and $(x)^{\uparrow}$ is a upward input. Both denote the communication between a child ambient and the parent ambient. Upward is the upward from the child to the parent. Whereas $< M >^n$ *or* $(x)^n$ is an output to or a input from a child ambient named ***n***.

3. NEEDHAM-SCHROEDER SYMMETRIC-KEY PROTOCOL

In [1], Roger Needham and Michael Schroeder have invented a symmetric-key protocol for mutual authentication. In this famous protocol, there are three parts: Alice, Bob, and Trent (a Server), and the mutual authentication among Alice and Bob could be established by the next five stages:

$$Stage\,1.\ Alice \rightarrow Trent : Alice, Bob, R_A$$
$$Stage\,2.\ Trent \rightarrow Alice : \{R_A, Bob, K, \{K, Alice\}_{K_B}\}_{K_A}$$
$$Stage\,3.\ Alice \rightarrow Bob : \{K, Alice\}_{K_B}$$
$$Stage\,4.\ Bob \rightarrow Alice : \{R_B\}_K$$
$$Stage\,5.\ Alice \rightarrow Bob : \{R_B - 1\}_K$$

In stage 1, Alice sends to Trent her name, the name of Bob, and R_A a randomly generated number (called nonce). In stage 2, Trent randomly generates a key *K*, encrypts the key *K* and the name of Alice using the key K_B shared by Trent and Bob, encrypts the nonce of Alice R_A, the name of Bob, the key *K*, and the cipher text $\{K, Alice\}_{K_B}$ using the key K_A shared by Trent and Alice, and finally sends the cipher text $\{R_A, Bob, K, \{K, Alice\}_{K_B}\}_{K_A}$ to Alice. After receiving the cipher text $\{R_A, Bob, K, \{K, Alice\}_{K_B}\}_{K_A}$ from Trent, Alice retrieves the Key *K* by decrypting the cipher text $\{R_A, Bob, K, \{K, Alice\}_{K_B}\}_{K_A}$ using the key K_A, verifies if the nonce retrieved from the same cipher text is the same as what she has sent to Trent, and finally sends the intact cipher text $\{K, Alice\}_{K_B}$ to Bob in stage 3. After receiving the cipher text $\{K, Alice\}_{K_B}$ resulting from the stage 3, Bob decrypts this cipher text, randomly generates a nonce R_B, encrypts the nonce R_B using the key *K* retrieved from the cipher text $\{K, Alice\}_{K_B}$, and finally sends the cipher text $\{R_B\}_K$ to Alice in stage 4. In stage 5, Alice decrypts the cipher text $\{R_B\}_K$ using the key *K*, and sends a new cipher text $\{R_B - 1\}_K$ to Bob. And finally, in stage 6, Bob decrypts the cipher text $\{R_B - 1\}_K$ sent by Alice in stage 5, and verifies whether or not its content is equal to $R_B - 1$. If this is the case, Bob and Alice are successfully mutually authenticated.

The troubles for the Needham-Schroeder symmetric-key protocol could come from an attack called replay attack. In [13], the authors have shown that, if "Mallory" has the key *K* and can capture the cipher text $\{K, Alice\}_{K_B}$ sent by Alice to Bob in stage 3, then Mallory can play the role in the place of Alice, and make Bob to believe that it is Alice. In [13, 14], the authors have found a method based on time-stamp to remedy this replay attack. Several ameliorations of the protocol can be found in [15, 16].

In this article, we are limited to specify the protocol presented in the original paper of Needham and Schroeder. Specification both of the enhanced protocol and of the attacks will be considered in our future works. In the next section, we formally describe the results of this article.

4. SPECIFICATION OF THE NEEDHAM-SCHROEDER SYMMETRIC-KEY PROTOCOL IN USING THE NBA

In this section, several special ambients are utilized to stand for processes running at different distributed location. Ambients ***A[P1|P2|……], Trent[P1|P2|……],*** and ***B[P1|P2|……]*** stand for the processes running at the location of Alice, Trent, and Bob, respectively, and these three ambients stay immobile. Ambient ***EKA[P1|P2|…]*** represents a ciphertext of a plaintext encrypted using the key K_A, the same signification for ambients ***EKB[P1|P2|…]*** and ***EK[P1|P2|…]*** unless the last two stand for cipher texts obtained by applying the keys K_B and *K* respectively. The ambient ***NonceGen[P1|P2|..]*** represents what from which Alice randomly generates a number as nonce, and ***NonceGen2[P1|P2|… …]*** is the same type of ambient for the side of Bob.

For specifying stage 1 of the Needham-Schroeder protocol, we have the next definition:

Definition 4-1. (Specification of the first stage of the Needham-Schroeder Protocol)

$$message1 \triangleq (\nu NonceGen)(\nu Lock1)(NonceGen[< R_A >^{\uparrow}]|$$
$$(n)^{NonceGen}.< n >^{m}.< n >^{AmbAliceNonce}.Lock1[< >^{\uparrow}]|$$
$$m[(x)^{\uparrow}.< x >^{q}|q[exit < m,k1 >|(y)^{\uparrow}.< y >^{\uparrow}.< Alice >^{\uparrow}.< Bob >^{\uparrow}]|$$
$$()^{Lock1}.exit < A,k1 >.enter < Trent,k1 >]|$$
$$AmbAliceNonce[(AliceNonce)^{\uparrow} < AliceNonce >^{\uparrow}]|\overline{exit}(x,k1))$$

$$\overline{message1} \triangleq \overline{enter}(x,k1).\overline{exit}(x,k1).(AliceNonce)^{x}.(AliceName)^{x}.$$
$$(BobName)^{x}.< AliceNonce >^{MessageAlice2Trent}.$$
$$< AliceName >^{MessageAlice2Trent}.< BobName >^{MessageAlice2Trent}.$$
$$Message_{Alice2Trent}[(AliceNonce)^{\uparrow}.(AliceName)^{\uparrow}.(BobName)^{\uparrow}.$$
$$< AliceNonce >^{\uparrow}.< AliceName >^{\uparrow}.< BobName >^{\uparrow}]$$

In the definition 4-1, the ambient ***AmbAliceNonce[P1|P2|…]*** is what in which Alice saves the nonce that She sends to Trent, the ambient $Message_{Alice2Trent}[P1 \mid P2 \mid ...]$ is the one used by Trent to store the message that He receives from Alice, and the ambient $m[P1 \mid q[P2 \mid P3]]$ wrappers the message sent by Alice and moves from Alice to Trent, please notice that the ambient $m[P1 \mid q[P2 \mid P3]]$ uses the password k1 to exit from Alice and to enter Trent. R_A stands for the nonce generated by Alice. The ambient $Lock1[...]$ represents a syntax sugar for synchronizing the movement of the message ambient $m[P1 \mid q[P2 \mid P3]]$. From the definition 4-1, we have the next proposition:

Proposition 4-1. (Specification of First stage of the Needham-Schroeder Protocol)

$$A[message1] \mid Trent[\overline{message1}] \cong$$
$$A[AmbAliceNonce[< R_A >^{\uparrow}]] \mid$$
$$Trent[Message_{Alice2Trent}[< R_A >^{\uparrow}.$$
$$< Alice >^{\uparrow}.< Bob >^{\uparrow}]]$$

The proposition 4-1 says that, the run of the processes $A[message1] \mid Trent[\overline{message1}]$ resulted to reception of a message containing the Alice name, the Bob name and the Alice nonce sent by Alice to Trent, and in addition Alice saved the nonce in the ambient ***AmbAliceNonce[…]***. This is exactly the result of the stage 1 of the Needham-Schroeder protocol.

For specifying the stage 2 of the Needham-Schroeder protocol, several special notations are utilized for encryption and decryption. $< Data >^{EKA}_{eka}$ signifies that we are encrypting the Data with the key K_A and writing the cipher text into the ambient EKA where store all cipher texts obtained by applying the key K_A, whereas $EKA[(Data)^{\uparrow}_{d}.P \mid Q]$ stands for that we are decrypting $(Data)^{\uparrow}_{d}$ using the K_A. We have the next definition:

Definition 4-2. (Specification of 2nd stage of the Needham-Schroeder Protocol)

$$message2 \triangleq (\nu Lock2)(\ KeyGen[< K >^{\uparrow}]|$$
$$(key)^{KeyGen}.(AliceNonce)^{Message}Alice2Trent.$$
$$(AliceName)^{Message}Alice2Trent(BobName)^{Message}Alice2Trent.$$
$$< AliceNonce >^{EKA}_{eka}.< BobName >^{EKA}_{eka}.< key >^{EKA}_{eka}.< key >^{EKB}_{ekb}.$$
$$< AliceName >^{EKB}_{ekb}.Lock2[< >^{\uparrow}]|EKB[(key)^{\uparrow}_{ekb}.(AliceName)^{\uparrow}_{ekb}.$$
$$enter < EKA,k2 >_{eka}.< key >^{\uparrow}_{d}.< AliceName >^{\uparrow}_{d}|exit < EKA,k2 >.$$
$$exit < A,k3 >.enter < B,k3 >]|EKA[(AliceName)^{\uparrow}_{eka}.(BobName)^{\uparrow}_{eka}.$$
$$(key)^{\uparrow}_{eka}.\overline{enter}(x,k2)_{eka}.< AliceNonce >^{\uparrow}_{d}.< BobName >^{\uparrow}_{d}.< key >^{\uparrow}_{d}|$$
$$()^{Lock2}.exit < Trent,k2 >.enter < A,k2 >]|\overline{exit}(x,k2))$$

$$\overline{message2} \triangleq \overline{enter}(x,k2).\overline{exit}(x,k2).(AliceNonceBack)^{EKA}_{d}.$$
$$(BobName)^{EKA}_{d}.(key)^{EKA}_{d}.< AliceNonceBack >^{Message}Trent2Alice.$$
$$< BobName >^{Message}Trent2Alice.< key >^{Message}Trent2Alice.$$
$$Message_{Trent2Alice}[(AliceNonceBack)^{\uparrow}.(BobName)^{\uparrow}.(key)^{\uparrow}.$$
$$< AliceNonceBack >^{\uparrow}.< BobName >^{\uparrow}.< key >^{\uparrow}]$$

In the definition 4-2, the ambient $KeyGen[< K >^{\uparrow}]$ signifies that in the stage 2 of the Needham-Schroeder protocol, Trent randomly generates a key K shared by its-self, Alice and Bob. The ambient $Message_{Trent2Alice}[Mess1.Mess2....]$ is the one of Alice for saving the messages she received from Trent. The ambient

$$EKA[P1|EKB[P2|exit < EKA,k2 >.exit < A,k3 >.$$
$$enter < B,k3 >]|()^{Lock2}.exit < Trent,k2 >.enter < A,k2 >]$$

uses the password *k2* to exit from Trent and enter into Alice, whereas the sub ambient $EKB[P2|exit < EKA,k2 >.exit < A,k3 >.enter < B,k3 >]$ uses the password *k2* to exit from its parent ambient, and *k3* to exit from Alice and enter into Bob for the next stage. Using different passwords can avoid the interference of the ambient' movement at different stages. From the definition 4-2, we can obtain the next result:

Proposition 4-2. (Specification of 2nd stage of the Needham-Schroeder Protocol)

$$A[message1|\overline{message2}]|Trent[\overline{message1}|message2] \cong$$
$$A[AmbAliceNonce[< R_A >^{\uparrow}]|EKB[< K >^{\uparrow}_{d}.< Alice >^{\uparrow}_{d}|$$
$$exit < A,k3 >.enter < B,k3 >]|$$
$$Message_{Trent2Alice}[< R_A >^{\uparrow}.< Bob >^{\uparrow}.< K >^{\uparrow}]]$$

The proposition 4-2 means that after running the first two stages of the Needham-Schroeder protocol, Alice received the message sent by Trent that is

$$EKA[< R_A >^{\uparrow}_{d}.< Bob >^{\uparrow}_{d}.< K >^{\uparrow}_{d}|$$
$$EKB[< K >^{\uparrow}_{d}.< Alice >^{\uparrow}_{d}|exit < A,k3 >.$$
$$enter < B,k3 >]]$$

, decrypted it with her key K_A, and retrieved the nonce that has been sent to Trent in the first stage, the name of Bob, and the key *K* generated by Trent which all are saved in the ambient $Message_{Trent2Alice}[< R_A >^{\uparrow}.< Bob >^{\uparrow}.< K >^{\uparrow}]$, and the cipher

text $EKB[< K >_d^{\uparrow} .< Alice >_d^{\uparrow} | exit < A,k3 > .enter < B,k3 >]$ being ready to be sent to Bob in the next stage. Please notice that the residue resulted from the stage 1 is $AmbAliceNonce[< R_A >^{\uparrow}]$, which is the ambient storing the nonce sent by Alice to Trent, and where Alice could retrieve the old nonce for comparing it with the new one sent by Trent. The proof for the proposition 4-1 could be found in the section appendix.

In the stage 3 of the Needham-Schroeder protocol, Alice sends the cipher text $EKB[< K >_d^{\uparrow} .< Alice >_d^{\uparrow} | exit < A,k3 > .enter < B,k3 >]$ to Bob. In order to achieve this, we define two new processes in the next definition:

Definition 4-3. (Specification of 3rd stage of the Needham-Schroeder Protocol)

$$message3 \triangleq \overline{exit}(x, k3)$$
$$\overline{message3} \triangleq enter(x, k3)$$

From the definition 4-3, we have the next proposition:

Proposition 4-3. (Specification of 3rd stage of the Needham-Schroeder Protocol)

$$A[message1 | \overline{message2} | message3] |$$
$$Trent[\overline{message1} | message2] | B[\overline{message3}]$$
$$\cong A[AmbAliceNonce[< R_A >^{\uparrow}]|$$
$$Message_{Trent2Alice}[< R_A >^{\uparrow} .< Bob >^{\uparrow} .< K >^{\uparrow}]|$$
$$B[EKB[< K >_d^{\uparrow} .< Alice >_d^{\uparrow}]]$$

Proposition 4-3 says that, Bob received from Alice the cipher text $EKB[< K >_d^{\uparrow} .< Alice >_d^{\uparrow}]$ that is ready to be decrypted by Bob using the key K_B.

In the stage 4 of the Needham-Schroeder protocol, Bob should randomly generate a nonce R_B, encrypts the nonce with the key *K*, and sends the cipher text $EK_{Bob2Alice}[< R_B >^{\uparrow}]$ to Alice. To be clearer, we have used the subscript Bob2Alice for indicating the direction of message flow. We have the next definition and proposition for specifying this stage:

Definition 4-4. (Specification of 4th stage of the Needham-Schroeder Protocol)

$$message4 \triangleq (\nu NonceGen2)(\nu Lock3)(NonceGen2[< R_B >^{\uparrow}] |$$
$$(key)_d^{EKB} .(AliceName)_d^{EKB} .< key >_p^{Message_{Alice2Bob3}} .$$
$$< AliceName >_p^{Message_{Alice2Bob3}} .(n)^{NonceGen2} .< n >_{ek}^{EK_{Bob2Alice}} .$$
$$< n >_p^{AmbBobNonce} ..Lock3[<>^{\uparrow}] |$$
$$Message_{Alice2Bob3}[(key)_p^{\uparrow} .(AliceName)_p^{\uparrow} .< key >_p^{\uparrow} .< AliceName >_p^{\uparrow}] |$$
$$| EK_{Bob2Alice}[(n)_{ek}^{\uparrow} .< n >_d^{\uparrow} | ()^{Lock3} .exit < B,k4 > .enter < A,k4 >])$$
$$| AmbBobNonce[(n)_p^{\uparrow} .< n >_p^{\uparrow}] | \overline{exit}(x, k4)$$
$$\overline{message4} \triangleq \overline{enter}(x, k4)$$

In the definition 4-4, the ambient $NonceGen2[< R_B >^{\uparrow}]$ signifies that Bob randomly generates a nonce R_B; the ambient $AmbBobNonce[(n)_p^{\uparrow} .< n >_p^{\uparrow}]$ is used to save the nonce; and the ambient $Message_{Alice2Bob3}[(key)_p^{\uparrow} .(AliceName)_p^{\uparrow} .< key >_p^{\uparrow} .< AliceName >_p^{\uparrow}]$ is used to save the decrypted message sent by Alice in the stage 3. The subscript in $(Data)_p^{\uparrow}$ signifies that the reading from the child ambient is protected. The cipher text $EK_{Bob2Alice}[< R_B >^{\uparrow}]$ in form of an ambient is using the password *k4* to exit from the Bob's immobile ambient and to enter into the Alice's immobile ambient. From the definition 4-4, we could conclude onto the proposition 4-4:

Proposition 4-4. (Specification of 4th stage of the Needham-Schroeder Protocol)

$$A[message1 | \overline{message2} | message3 | \overline{message4}] |$$
$$Trent[\overline{message1} | message2] | B[\overline{message3} | message4]$$
$$\cong A[AmbAliceNonce[< R_A >^{\uparrow}] | EK_{Bob2Alice}[< R_B >^{\uparrow}] |$$
$$Message_{Trent2Alice}[< R_A >^{\uparrow} .< Bob >^{\uparrow} .< K >^{\uparrow}] |$$
$$B[Message_{Alice2Bob3}[< K >_p^{\uparrow} .< Alice >_p^{\uparrow}] |$$
$$AmbBobNonce[< R_B >^{\uparrow}]]$$

Proposition 4-4 says that, after executing the first four stages of the Needham-Schroeder protocol, at the party of Alice, she keeps not only the residues issued from the stages 1 and 2 which respectively are $AmbAliceNonce[< R_A >^{\uparrow}]$ and $Message_{Trent2Alice}[< R_A >^{\uparrow} .< Bob >^{\uparrow} .< K >^{\uparrow}]$, but also the nonce of Bob encrypted with the key K, $EK_{Bob2Alice}[< R_B >^{\uparrow}]$, that she just received in the stage 4; while at the party of Bob, he keeps the tracks of the message

sent by Alice in the previous stage that is $Message_{Alice2Bob3}[< K >^{\uparrow}_{p} . < Alice >^{\uparrow}_{p}]$, and of the nonce saved in the ambient $AmbBobNonce[< R_B >^{\uparrow}]$.

In the 5th stage of the Needham-Schroeder protocol, after having received the nonce of Bob in the previous stage, Alice decides to randomly generate a new nonce equal to $R_B - 1$, and sends the new nonce to Bob. For specifying this stage, we give the next definition:

Definition 4-5. (Specification of 5th stage of the Needham-Schroeder Protocol)

$$message5 \triangleq (\nu Lock4)((BobNonce)_{d}^{EK_{Bob2Alice}} .$$
$$< BobNone - 1 >_{ek}^{EK_{Alice2Bob5}} .$$
$$< BobNone - 1 >_{ek}^{AmbAliceNewNonce} .Lock4[<>^{\uparrow}] \mid$$
$$AmbAliceNewNonce[(AliceNewNonce)^{\uparrow}_{p}. < AliceNewNonce >^{\uparrow}_{p}] \mid$$
$$EK_{Alice2Bob5}[(AliceNewNonce)^{\uparrow}_{ek} . < AliceNewNonce >^{\uparrow}_{d} \mid$$
$$()^{Lock4}.exit < A, k5 > .enter < B, k5 >] \mid \overline{exit}(x, k5))$$
$$\overline{message5} \triangleq \overline{enter}(x, k5)$$

In this stage of the protocol, the new nonce of Alice is encrypted by the key *K*, and transported under the cipher text in form of the ambient $EK_{Alice2Bob5}[< R_B - 1 >^{\uparrow}]$. The new nonce of Alice, in the same time, is saved in the ambient $AmbAliceNewNonce[< R_B - 1 >^{\uparrow}]$. From the definition 4-5, we could obtain the next proposition:

Proposition 4-5. (Specification of 5th stage of the Needham-Schroeder Protocol)

$$A[message1 \mid \overline{message2} \mid message3 \mid \overline{message4} \mid message5] \mid$$
$$Trent[\overline{message1} \mid message2] \mid B[\overline{message3} \mid message4 \mid \overline{message5}]$$
$$\cong A[AmbAliceNonce[< R_A >^{\uparrow}] \mid AmbAliceNewNonce[< R_B - 1 >^{\uparrow}] \mid$$
$$Message_{Trent2Alice}[< R_A >^{\uparrow} . < Bob >^{\uparrow} . < K >^{\uparrow}]] \mid$$
$$B[Message_{Alice2Bob3}[< K >^{\uparrow}_{p} . < Alice >^{\uparrow}_{p}] \mid$$
$$AmbBobNonce[< R_B >^{\uparrow}] \mid EK_{Alice2Bob5}[< R_B - 1 >^{\uparrow}]]$$

We could simply say that the run of the first five stages of the Needham-Schroeder protocol is well formally specified by the proposition 4-5.

The last stage of the run of the protocol is that, Bob decrypts the new nonce of Alice sent in the previous stage, and verifies whether or not it is equal to $R_B - 1$. If this is case, then Alice and Bob have been successfully mutually authenticated. For specifying the last stage of the protocol, we give the definition 4.6, and the result of this article:

Definition 4-6. (Specification of 6th stage of the Needham-Schroeder Protocol)

$$message6 \triangleq (AliceNewNonce)_{d}^{EK_{Alice2Bob5}} .$$
$$< AliceNewNonce >_{p}^{Message_{Alice2Bob5}} \mid$$
$$Message_{Alice2Bob5}[(AliceNewNonce)^{\uparrow}_{p}. < AliceNewNonce >^{\uparrow}_{p}]$$

Lemma 4-1. (Formal Specification of the Needham-Schroeder Protocol)

$$A[message1 \mid \overline{message2} \mid message3 \mid \overline{message4} \mid message5] \mid$$
$$Trent[\overline{message1} \mid message2] \mid B[\overline{message3} \mid message4 \mid \overline{message5} \mid$$
$$message6] \cong A[AmbAliceNonce[< R_A >^{\uparrow}] \mid$$
$$AmbAliceNewNonce[< R_B - 1 >^{\uparrow}] \mid$$
$$Message_{Trent2Alice}[< R_A >^{\uparrow} . < Bob >^{\uparrow} . < K >^{\uparrow}]] \mid$$
$$B[Message_{Alice2Bob3}[< K >^{\uparrow}_{p} . < Alice >^{\uparrow}_{p}] \mid$$
$$AmbBobNonce[< R_B >^{\uparrow}] \mid Message_{Alice2Bob5}[< R_B - 1 >^{\uparrow}]]$$

The proof of the Lemma 4-1 is similar to that of the propositions of 4-1 and omitted here.

5. RELATED WOKS

In [6], authors have specified the Needham-Schroeder symmetric-key protocol using the classical process algebra CSP [5]. In [4], the same protocol has been specified and verified by the SPI calculus [3] that is a process algebra specially conceived for specification and verification of transport or cryptographic protocols. While in [17], the authors have carried out the same work by means of the process algebra μ CRL. In [18], C. Braghin et al. have tried specified a fragment of the Needham-Schroeder symmetric-key protocol using the pure mobile ambient (MA), but the non-determinism and the interference of movement of ambients due to the limitation of MA, has made the specification of the protocol to be very complex and semi-formal. We believe that our effort in this article is a utile attempt of specifying protocols by a variant of MA.

6. CONCLUSIONS

In this article, we use a variant of the mobile ambient to specify the famous Needham-Schroeder symmetric-key cryptographic protocol. The specification has been proven to be well formed. The extension of Boxed Ambient, NBA, is a tool suitable to specify protocols.

REFERENCES

[1] R.M. Needham and M. D. Schroeder,"Using encryption

for authentication in large networks of computers," *Comm. ACM*, Vol.21,No.12,pp.993-999,1978.

[2] T. Coffey, and P. Saidha,"Logic for verifying public-key cryptographic protocols,"*IEE Proceedings - Comput. Digit. Tech.*, Vol. 144, No. 1, 1997.

[3] M. Abadi and A. D. Gordon,"A calculus for cryptographic protocols: The spi calculus,"in *4th ACM Conference on Computer and Communications Security*, ACM, 1997.

[4] M. Bugliesi, R. Focardi, and M. Maffei,"Principles for entity authentication,"*in Proc. of 5th International Conference Perspectives of System Informatics (PSI 2003)*, vol. 2890, pp. 294–307, 2003.

[5] C. A. R. Hoare. *Communicating Sequential Processes*. Prentice-Hall International, 1985.

[6] G. Lowe,"Breaking and fixing the Needham-Schroeder public-key protocol using CSP and FDR,"in T. Margaria and B. Steffen, editors, *Tools and Algorithms for the Construction and Analysis of System, Second International Workshop, TACAS' 96*, LNCS 1055, pp. 147-166, 1996.

[7] L. Cardelli and A. Gordon,"Mobile Ambients,"in *Proceedings of POPL '98*. ACM Press, 1998.

[8] M. Bugliesi, G. Castagna, and S. Crafa,"Boxed Ambients,"*in Proceedings of TACS '01*, number 2215 in Lecture Notes in Computer Science, pp. 38-63, Springer, 2001.

[9] S. Crafa, M. Bugliesi, and G. Castagna,"Information Flow Security for Boxed Ambients,"*in F-WAN: Int. Workshop on Foundations of Wide Area Network Computing*, ENTCS 66.3, Elsevier, 2002.

[10] A. Philips. *The Channel Ambient Calculus: From Process Algebra to Mobile Code*. PhD thesis, Imperial College London, 2004.

[11] J. Vitek and G. Castagna,"Seal: A framework for secure mobile computations," in *Internet Programming Languages*, number 1686 in Lecture Notes in Computer science. Springer, 199.

[12] F. Levi and D. Sangiorgi,"Controlling Interference in Ambients," *in Proceedings of POPL'00*, pp. 352-364, ACM Press, 2000.

[13] D. E. Denning and G. M. Sacco, "Time-stamps in Key Distribution Protocols," *Communications of the ACM*, vol. 24, No.8, pp. 533-536, 1981.

[14] D. E. Denning, *Cryptography and Data Security*, Addison-Wesley, 1982.

[15] K. R. Bauer, T. A. Bersen, and R. J. Feiertag,"A Key Distribution Protocol Using Event Markers," *ACM Transactions on Computer Systems*, vol. 1, No.5, pp. 249-255, 1983.

[16] R. M. Needham and M. D. Schroeder, "Authentication Revisited," *Operating Systems Review*, vol. 21,No.1, pp. 7, 1987.

[17] J. Pang, "Analysis of a security protocol in μ CRL, "*in Proc. 4th Conference on Formal Engineering Methods*, LNCS 2495, pp. 396-400. Springer, 2002.

[18] C. Braghin, A. Cortesi and R. Focardi,"Freshness Analysis in Security Protocols in Mobile Ambient Calculus," *Proc. Of 14th Nordic Workshop on Programming Theory (NWPT'02)*, 2002, pp. 30-33.

APPENDIX

Proof for Proposition 4-1.

See the next figure for the Proof for the Proposition 4-1. Proofs for other conclusions are similar as for the one of the Proposition 4-1, so omitted.

$$
\begin{aligned}
&message1 \rightarrow (\nu NonceGen)(\nu Lock1)(NonceGen[] \mid \\
&<R_A>^{m}.<R_A>^{AmbAliceNonce}.Lock1[<>^{\uparrow}] \mid \\
&m[(x)^{\uparrow}.<x>^{q} \mid q[exit<m,k1> \mid (y)^{\uparrow}.<y>^{\uparrow}.<Alice>^{\uparrow}. \\
&<Bob>^{\uparrow}]] \mid ()^{Lock1}.exit<A,k1>.enter<Trent,k1>] \mid \\
&AmbAliceNonce[(AliceNonce)^{\uparrow}.<AliceNonce>^{\uparrow}] \mid \\
&\overline{exit}(x,k1)) \rightarrow (\nu NonceGen)(\nu Lock1)(NonceGen[] \mid \\
&<R_A>^{AmbAliceNonce}.Lock1[<>^{\uparrow}] \mid \\
&m[<R_A>^{q} \mid q[exit<m,k1> \mid (y)^{\uparrow}.<y>^{\uparrow}.<Alice>^{\uparrow}. \\
&<Bob>^{\uparrow}]] \mid ()^{Lock1}.exit<A,k1>.enter<Trent,k1>] \mid \\
&AmbAliceNonce[(AliceNonce)^{\uparrow}.<AliceNonce>^{\uparrow}] \mid \\
&\overline{exit}(x,k1)) \rightarrow (\nu Lock1)(0 \mid Lock1[<>^{\uparrow}] \mid \\
&m[q[exit<m,k1> \mid <R_A>^{\uparrow}.<Alice>^{\uparrow}.<Bob>^{\uparrow}] \mid \\
&()^{Lock1}.exit<A,k1>.enter<Trent,k1>] \mid \\
&AmbAliceNonce[<Alice>^{\uparrow}] \mid \overline{exit}(x,k1)) \\
&\Rightarrow m[q[exit(m,k1) \mid <R_A>^{\uparrow}.<Alice>^{\uparrow}.<Bob>^{\uparrow}] \mid \\
&exit<A,k1>.enter<Trent,k1>] \mid \\
&AmbAliceNonce[<Alice>^{\uparrow}] \mid \\
&\overline{exit}(x,k1)) \\
&A[message1] \Rightarrow A[m[q[exit(m,k1) \mid \\
&<R_A>^{\uparrow}.<Alice>^{\uparrow}.<Bob>^{\uparrow}] \mid \\
&exit<A,k1>.enter<Trent,k1>] \mid \\
&AmbAliceNonce[<Alice>^{\uparrow}] \mid \overline{exit}(x,k1)] \\
&\rightarrow A[AmbAliceNonce[<Alice>^{\uparrow}]] \mid \\
&m[q[exit<m,k1> \mid <R_A>^{\uparrow}.<Alice>^{\uparrow}. \\
&<Bob>^{\uparrow}] \mid enter<Trent,k1>]
\end{aligned}
$$

$$
\begin{aligned}
&A[message1] \mid Trent[\overline{message1}] \Rightarrow \\
&A[AmbAliceNonce[<Alice>^{\uparrow}]] \mid \\
&Trent[m[q[exit<m,k1> \mid <R_A>^{\uparrow}.<Alice>^{\uparrow}.<Bob>^{\uparrow}]] \mid \\
&\overline{exit}(x,k1).(AliceNonce)^{x}.(AliceName)^{x}.(BobName)^{x}. \\
&<AliceNonce>^{Message_{Alice2Trent}}. \\
&<AliceName>^{Message_{Alice2Trent}}. \\
&<BobName>^{Message_{Alice2Trent}}. \\
&Message_{Alice2Trent}[(AliceNonce)^{\uparrow}.(AliceName)^{\uparrow}. \\
&(BobName)^{\uparrow}.<AliceNonce>^{\uparrow}.<AliceName>^{\uparrow}. \\
&<BobName>^{\uparrow}]] \rightarrow A[AmbAliceNonce[<Alice>^{\uparrow}]] \mid \\
&Trent[m[] \mid q[<R_A>^{\uparrow}.<Alice>^{\uparrow}.<Bob>^{\uparrow}] \mid \\
&(AliceNonce)^{q}.(AliceName)^{q}.(BobName)^{q}. \\
&<AliceNonce>^{Message_{Alice2Trent}}. \\
&<AliceName>^{Message_{Alice2Trent}}. \\
&<BobName>^{Message_{Alice2Trent}}. \\
&Message_{Alice2Trent}[(AliceNonce)^{\uparrow}.(AliceName)^{\uparrow}.(BobName)^{\uparrow}. \\
&<AliceNonce>^{\uparrow}.<AliceName>^{\uparrow}.<BobName>^{\uparrow}]] \\
&\Rightarrow A[ANonce[<Alice>^{\uparrow}]] \mid Trent[\\
&Message_{Alice2Trent}[<R_A>^{\uparrow}.<Alice>^{\uparrow}.<Bob>^{\uparrow}]]
\end{aligned}
$$

Research on a Distributed Spam Filtering System

Qiuyu Zhang[1], Jingtao Sun[1], Wenhan Huang[2]
[1]School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, Gansu Province, China
[2]Department of Computer science and technology, Shaanxi University of Technology, Hanzhong, 723003, China
Email: [1]1sun2651@mail2.lut.cn, [2]zhangqy@lut.cn

ABSTRACT

The spam problem has been becoming widely concerned gradually. Due to that the spam filtering systems between the server and customer can't cooperate, the filter rules of spam filtering system can't be dynamic changed. This paper is to propose a model of Distributed Spam Detection, making use of the Distributed network technique to resolve cooperation between systems. Making use of the Pattern matching and BP neural network technique, this model can be used to resolve the problem that the filter rules of spam filtering system can't be dynamic changed. Based on this model it is designed a Distributed Spam Filtering System, and the architecture of the system and the implement have been discussed in details. The experiments show the feasibility and advantage of the new Spam Filtering method, which is better than some traditional anti-spam skills and can realize efficient spam detection in distributed and isomerous networks.

Keywords: Spam, Pattern Matching, BP Neural Network, Behavior Characteristic Matching

1. INTRODUCTION

The spam mainly includes: all kinds of Commercial advertisements and the network advertisements of lawless groups, email virus. It is a waste of the limited network resource, jamming network, breaking computer system seriously [1,2] and causing a severe loss in economy. Therefore, the spam detection has significant application, becoming a hot research problem in recent years. The research in this area comes in two main types [3]: client-side and server-side. But most of existing spam filtering systems in client-side and server-side work independently, i.e., they cannot cooperate as a whole system. When the quantity of spam increases, this kind of independent spam filtering systems will hardly apply. Currently, the spam filtering system needs to change the detection rules artificially to adapt each kind of environment. This method is difficult to meet the users' needs when spam's character is changing continuously. It is necessary to introduce new technique and modify present related schemes to resolve the above problem.

2. DISTRIBUTED SPAN FILTERING SYSTEM ANALYSIS

Currently, the Distributed Spam Filtering System is still in a developed stage. With the popularity of Internet, by employing Distributed network technique and Spam Filtering technique it is possible to make most existing spam filtering systems of client-side and server-side work as a whole, so achieve information sharing and cooperating of two C/S sides.

Analyzing the problem of Distributed Spam Filtering System thoroughly, it is seen that Spam Filtering is essentially classification problem, with nonlinear and nondeterministic character. The classification problem can be solved by using Back-Propagation Neural Networks (BPN) and Pattern matching. So employing these methods, we will design a Distributed Spam Filtering system, called DSFS (Distributed Spam Filtering System) to solve spam filtering problem.

3. KEY TECHNICAL ANALYSIS

3.1 Pattern Matching

Pattern matching is a basic Pattern recognition method [4, 5], which studies how to use computer to realize the human capability of pattern recognition. Based on statistic learning model, there are four steps in pattern matching: data acquisition, preprocess, character extraction and selection, and category decision [6], as shown in Fig.1.

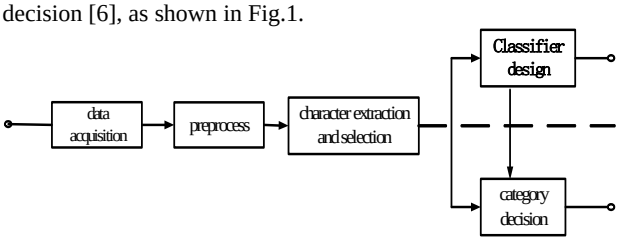


Fig.1. Pattern recognition system

1) Data acquisition is the procedure to acquire computable symbols by using the methods of measuring, sampling, quantifying and etc., for efficient Pattern matching;
2) Preprocess is a procedure to remove noise in data and strengthen useful information;
3) Character extraction and selection is a procedure to transform the data then select essential characters for effectively realizing Pattern matching;
4) Category decision is to classify an object into a special Category class by statistic methods in the characteristic space.

Generally, the pattern matching is usable to classify an object to a special class. The usage is needed in the spam detection. So, the pattern matching method can be employed for spam detection.

3.2 BP Neural Networks

An artificial neural network is an intelligent universal mechanism of dealing with pattern recognition, process estimation and prediction, optimization design and other applications [7]. In 1986, BPN is put forward by Rumelhart and LeCun et al., which is one of such artificial neural network mechanisms [8]. It overcame the big obstacles which baffled the development of the perceptron models, so was an important breakthrough in the history of the theory and application of neural networks. A BPN is a layered network consisting of an input layer, an output layer, and at least one nonlinear processing layer. Its main idea is to propagate back error of output layer; the error of hidden layer is calculated indirectly. The classifying procedure of neural network is divided into two stages: the first stage (forward-propagation), the BPN propagates its input vectors, which can be any multivariate data series, to its output layer through a series calculation. The second stage (back-propagation), the error of each layer is

calculated by back-propagation error of output layer. The preceding layer weight is adjusted by the error of every layer [9]. The procedure is shown in Fig.2. Investigate the *j*th calculation unit of one layer, label *i* is the *i*th unit of its frontal layer; label *k* is the *k*th unit of latter layer; o_j is the output of current layer; ω_{ij} is the weight from preceding layer to current layer. ω_{jk} is the weight from latter layer to current layer.

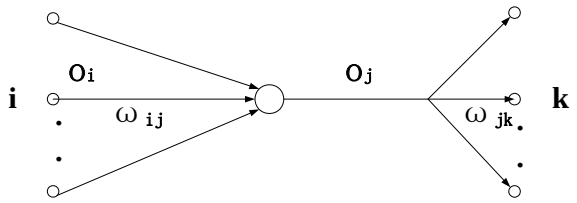


Fig.2.

The calculation steps are [10]:

1) Select the initial value of weight ω_{ij};
2) Repeat the below process until convergence (recurse on each sample).
   (1) Compute every unit o_j in turn.

$$net_j = \sum_i \omega_{ij} o_i$$

   Where $o_j = f(net_j)$, f is unsymmetrical Sigmoid function.

   (2) The output layer is calculated as:

$$\delta_j = (y - o_j) o_j (1 - o_j)$$

   (3) Every hidden layer is calculated as:

$$\delta_j = o_j (1 - o_j) \sum_k \omega_{jk} \delta_k$$

   (4) Calculate and save the revised weights:

$$\Delta \omega_{ij}(t) = \alpha \Delta \omega_{ij}(t-1) + \eta \delta_j o_i$$

   (5) Revise the weights:

$$\omega_{ij}(t+1) = \omega_{ij}(t) + \Delta \omega_{ij}(t)$$

   (6) After every weight of layer has been calculated, these weights were judged whether to satisfy the request according to known condition. If the request is satisfied, the algorithm ends; if not then repeat from the step i.

A BPN is applied to the nonlinear self-tuning tracking problem. The neural network has a strong ability of study and large-scale Parallel Computing. It can effectively handle the problem that the spam character is changing continuously; it makes the system to carry on a continuous self-study with the changing email character, so realizes the intelligence of email filtering at last.

4. DISTRIBUTED SPAM FILETERING SYSTEM MODEL

4.1 DSFS System Structure

The DSFS is an integral system to collect email characters, analyze and filter emails. In the system the client-side detection and server-side detection are combined together. The system can be used to the networked structure and distributed spam filtering. The DSFS is made up of central management node, client-side detection node and server-side detection node, as shown in Fig.3. The DSFS can include several server-side detection nodes and client-side detection nodes, but only one central management node.

The server-side (client-side) detection nodes collect original data related emails, extract the characters of the original data according to the customer requests, then feedback the extracted information to management node, so the real-time condition control is accomplished in the system. The original data characters are analyzed at the server-side (client-side) detection nodes; the results are reported to central management node. A server-side (client-side) detection node consists of six parts: server-side (client-side) manager, email character collection module, email character extraction module, email character analysis module, repository and email disposal module.

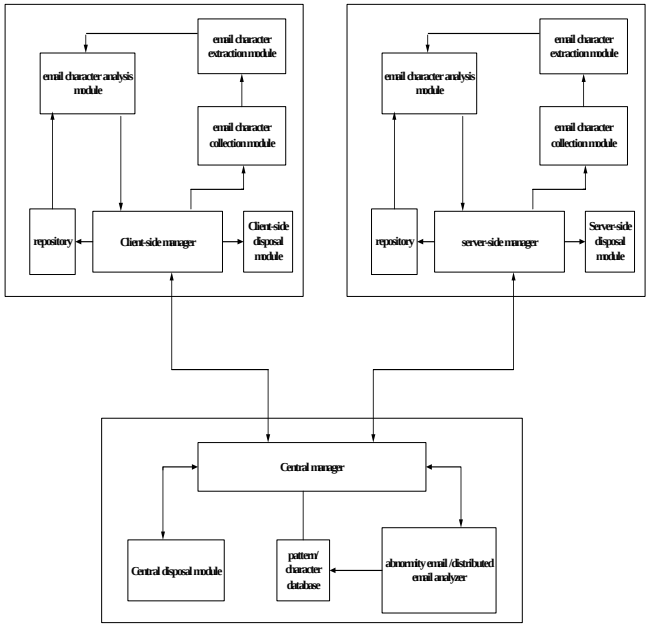


Fig.3. System structure

All server-side (client-side) detection nodes are managed by central management node. The central management node is responsible for monitoring the communication between itself and every detection node. The data reported from each node is collected and stored. All these data are categorized and carried on abnormity analysis. A central management node consists of four parts: central manager, central disposal module, pattern/character database, and abnormity email /distributed email analyzer.

4.2 Design of Each Part Of DSFS

4.2.1 Email character analysis module

Currently, the Pattern matching is already one of matured technique. Using the technique, the spam can be identified from the email content characters and the behavior characters of sending out. The technique can be adopted in the DSFS system as following:

1) The spam is judged by some content characters.
2) The spam is judged by one or some of the following specific behaviors:
   (1) The email with over issued behavior: the maker of spam has on-line query and deliver email at landing server, trying various way to deliver email, the host of sending out email changes behavior unusually, etc..
   (2) The email with illegal behavior: the maker of spam has behavior of sending out email by making use of Open Relay function of many possible email servers.
   (3) Email sender, receiver, host of sending email or email

information are intentionally hided, these behaviors make it difficult to trace the email source.

(4) The behavior of forging email: sender, receiver, host of sending email or email information are intentionally forged, which don't belong to honest behaviors through the identification.

The DSFS system adopts the detection technique of the Pattern matching, with some advantages such as: it detects the spam with known characters with high accuracy and efficiency, so can deal with the detected spam at real time. But it has weakness that it depends on the complete and the accurate modes of the spam detection in the knowledge database. For improving detection accuracy, the system announces the new spam characters from the Central disposal module to server-sides and client-sides to renew the knowledge database of the detection modes dynamically.

4.2.2 Analyzer of email abnormity

The analyzer of email abnormity is constructed based on BP neural network technique. By this technique, the DSFS system can improve ability to identify unknown spam and new transformations of previously known spam.

1) The design of the analyzer based on BP neural network

In order to adopting the BP neural network technique, we need to train applicable BP neural network. But the function of BP neural network is closely related to its input, layer number, neural cell number of every layer and initial weight values etc. The main problem during the BP neural network training is uncertainty of its hidden layer. In addition, the knowledge of neural network is mainly decided by threshold values of nodes and weight values of network conjunctions, these values not only influence convergence speed of network, but also may influence the function of final network evidently.

Based on the above consideration, for better performance of BP neural network, in this paper the neural network of 3 layers (input layer, hidden layer and output layer) is adopted, and the analyzer of 3 layered neural networks is designed as following [11]:

(1) Input/output layer [12] :

In the Distributed Spam Filtering System, the input signal of neural network comes from Pattern/character pick-up module. In this way, the difficulty of choosing neural cell number of input layer is reduced. The analyzer of neural network carries out the discrimination of abnormality/normality. Combining all these factors, a neural network is constructed with the neural cell number of its input layer as *n*, this the number of characters extracted by Pattern /character pick-up module, and the neural cell number of its output layer as 2.

(2) Hidden layer [13]

In the hidden layer of the neural network, a very difficult problem is the choice of the neural cell number, it is usually determined by experience and experiment result. Based on some known results, we carry on a design according to the following formula:

$$N_{\mathrm{H}} = (N_{\mathrm{In}} + \max(N_{out}, N_c)) / 2$$

Where N_{H} is the node number of the hidden layer, N_{In} is the node number of input layer, N_{out} is the node number of output layer, N_c is the number of classification.

Fig.4 is experiment result with different hidden layer node number. The hidden layer node number is closely related with the need of problem and input/output cell number. When hidden layer node number is n<6, the result of the mean square error is bigger; when hidden layer node number is n>6, the result of the mean square error is not minimum, Therefore, we select n=6.

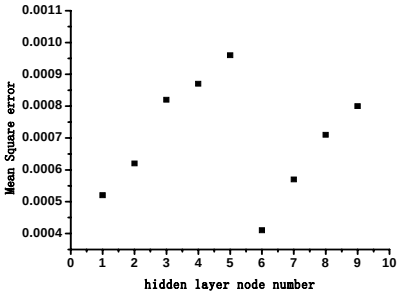


Fig.4. Hidden layer node number

(3) initial weight value selection [14,15]

At present, the network weight values and network threshold values are initialized randomly in (- 1, 1).

2) Analyzer of email abnormity:

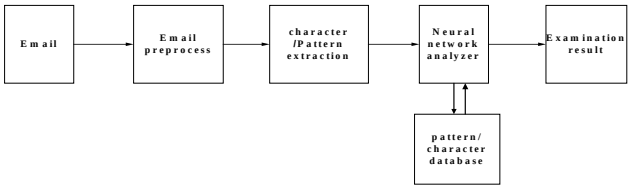


Fig.5. Analyzer of email abnormity

Fig 5 is design of analyzer of email abnormity; it is constructed based on neural network. Its working flow: ①email preprocess; ②extract modes/characters, then convert them into input for the neural network, ③compute the input through the neural network;④ if one email is judged as spam, then notify Central disposal module;⑤the Pattern/characteristic information will be saved in Pattern/Characteristic database if it is new one.

4.3 Email Disposal Module

The email disposal module mainly carries on a process to the spam which examines:

1) Client-side carries on putting the suspicious spam into a garbage box of Client-side, deleting after receiving customer's confirmation.
2) Server-side carries on putting the suspicious spam into the garbage box of server-side, after examining through managing person, if it is a spam, it will be deleted, otherwise it will be recover.
3) At central management node, a new discovered character of the spam will be announced to server-side and client-side by the central manager.

5. THE EXPERIMENT

We build up a network environment to implement experiment. There are many choices for the data set, such as Spamassassin, etc., but there is no authorized standard for data set of E-mails in Chinese. We have stochastically collected 3500 spam and 150 normal email of each kind, with 35MB as training set. Data

type and attribute are shown below:

number \ type	Normal	SPAM
training sets	100	2600
Testing sets	50	900

The performance of the Spam Filtering System is evaluated by the following 3 guide lines.

1) The recall is spam detection rate. This guide line reflects system ability to discover spam. The recall is higher, the non-detected spam are less accordingly.
2) The Precision is right rate at which spam are judged. This guide line reflects system ability to discover spam rightly. The Precision is higher, the normal emails are less judged as spam accordingly.
3) F value is harmonic mean of the recall and precision.

The formulas are as following:

Recall: $R = \frac{N_A}{N_S} \times 100\%$;

Precision: $P = \frac{N_A}{N_A + N_B} \times 100\%$;

F value: $F = \frac{2RP}{R+P} \times 100\%$

where N_A is number of spam which are judged correctly; N_S is number of actual spam; N_B is number of normal email that are judged as spam.

The filtered result got by the DSFS:

Test type \ Fact type	Normal	SPAM	Recall	Precision	F value
Normal	37	33	96.33%	98.5%	97.4%
SPAM	31	867			

The filtered result got by the system based on Naïve Bayes technique with same test sets.

Test type \ Fact type	Normal	SPAM	Recall	Precision	F value
Normal	20	303	77.51%	95.87%	85.71%
SPAM	30	697			

As shown in the tables, the Recall rate is increased 18.82% by using the DSFS model, the Precision rate is increased 2.63%, and the F1 value is increased11.69%.

In order to further state the superiority of DSFS comparing with Naïve Bayes technique, we show the tendencies of F values of two methods as the collected email data is increasing, as shown in Fig.6. The DSFS exhibits good application result.

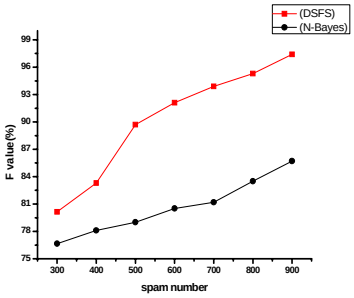


Fig.6. F values

6. CONCLUSIONS

The spam filtering techniques play an important role in improving the email safety and blocking the spam dissemination. The DSFS can carry on a spam detection based on Pattern matching technique. The system has high efficiency, fast speed, high accuracy and real time etc. The DSFS can also carry on Abnormity email detection based on BP neural network technique, the system can discover unknown characters of spam. The DSFS can adapt network processing request based on Distributed technique. Certainly, the system still needs more research, to increase intelligence of the whole system, improve the accuracy of spam detection, etc.

REFERENCES

[1] Hoanca B." How good are our weapons in the spam wars?" *Technology and Society Magazine, IEEE Technology and Society Magazine*, IEEE, 2006, 25(1): 22- 30.
[2] Deepak P, Sandeep P. "Spam filtering using spam mail communities," *Applications and the Internet*, pp. 377-383, 2005.
[3] Garg A, Battiti R, Cascella R G. "May I borrow your filter?" Exchanging filters to combat spam in a community. *Advanced Information Networking and Applications*, pp.5, 2006.
[4] Stanojevic M, Vranes S, Velasevic D. "Pattern matching in search problem solving," *System Sciences*, pp. 201-209 vol.2, 1996.
[5] Tao T, Amar M. "Pattern matching in LZW compressed files," *IEEE Transactionon Computers*, 2005, 54(8): 929- 938.
[6] Ruspini E H, Thomere J, Wolverton M. "Database editing metrics for pattern matching," *Computational Intelligence for Homeland Security and Personal Safety*, pp. 31- 38, 2004.
[7] *Proceedings of the 2002 International Joint Conference on Neural Networks*, IJCNN'02 (Cat. No.02CH37290), 2002.
[8] Chen F -, "Back-propagation neural networks for nonlinear self-tuning adaptive control," *Control Systems Magazine, IEEE Control Systems Magazine*, IEEE. 1990, 10(3): 44-48.
[9] Jeng-bin L, Yun-kung C, "A Novel Back-propagation Neural Network Training Algorithm Designed by an Ant Colony Optimization," *Transmission and Distribution Conference and Exhibition*, pp. 1- 5, 2005.
[10] Ramasubramanian P, Kannan A, "Intelligent multi-agent based back-propagation neural network forecasting model for statistical database anomaly prevention

system," *Intelligent Sensing and Information Processing*, pp.108- 113, 2004.
[11] Guowei H, Hall G, Terrell T, "Prediction by back-propagation neural network for lossless image compression," *Signal Processing*, pp. 1026- 1030 vol.2, 1996.
[12] Min H, Lei C, Hua M, "Application of four-layer neural network on information extraction," *Neural Networks*, pp .2146- 2151 vol.3, 2003.
[13] Burke H B, Rosen D B, Goodman P H. "Comparing artificial neural networks to other statistical methods for medical outcome prediction," *Neural Networks*, pp.2213-2216 vol.4, 1994.
[14] Antsaklis P J. "Neural networks for control systems, Neural Networks," *IEEE Transactions on Neural Networks*, IEEE Transactions on, 1990, 1(2): 242- 244.
[15] Abou-nasrm A.S A, "Fast Learning and Efficient Memory Utilization with a Prototype Based Neuron-Classifier,"*Pattern Recognition*.pp.32, 1995.

Qiuyu Zhang: Associate professor and master tutor. Vice dean of School of computer and communication in Lanzhou University of Technology, director of software engineering center, vice dean of Gansu manufacturing information engineering research center, director of "software engineering" characteristic research direction and academic group of Lanzhou University of Technology. His research interests include: image processing and pattern recognition, multimedia information processing, information security, software engineering etc.

Jingtao Sun: Graduate student. Born in DaQing Heilongjiang province in 1981, have published many academic papers in domestic core magazine and international conference. His research interests include: information security, Chinese text classification, Anti-Spam etc.

Design of Distributed Heterogeneous Anti-Money Laundering System based on Multi-Agent*

Qifeng Yang, Bin Feng, Ping Song
Economics College, Wuhan University of Technology
Wuhan, Hubei, 430070, P.R.China
Email: yangqifengwhut@163.com, 13027154642@vip.163.com, songpingwhut@163.com

ABSTRACT

Money laundering by e-commerce becomes more and more prevalent and serious, and harms the financial market and the economic order. In order to help the anti-money laundering (AML) carry on efficiently, we designed a distributed heterogeneous AML system which works during the process of online payment. This system used several agent such as data mining agent, case-based reasoning agent, neural network agent and genetic algorithm agent to monitor the transaction data. By tracing and analyzing the capital flow route, this system collects the relevant rule of the transaction and experience in AML area, processes these information into the form of knowledge which the user can identify, and stores them into the knowledge base. Each agent filters the input data one by one under the conduct of knowledge base, and judges the transaction behavior by matching its inherent condition. This AML system improves the ability of disguising the money laundering behavior from the online transaction greatly.

Keywords: Anti-Money laundering, Multi-Agent, Distributed, Data Mining, Online Payment

1. INTRODUCTION

With the fast development of the computer and network technology, e-commerce has brought a lot of new challenges while bringing great convenience for us. Because of its characteristics such as no paper, no boundary, no address, and the faultiness of the relevant law and management system, e-commerce becomes one of important means to launder money gradually. The amount of money laundered by e-commerce are increasing year by year, however, there is few efficient anti-money laundering (AML) mechanism nowadays. In this paper, an AML system based on union-bank online payment mode was introduced. This system can monitor the capital flow and information flow during the process of online payment, and improve the ability to identify the money laundering behavior effectively.

2. SYSTEM CHARACTERISTICS

The distributed heterogeneous AML system based on Multi-Agent has the following characteristics.

(1) The system can be used independently, but it's suggested being used under the union-bank online payment mode. The union-bank online payment is a solution scheme proposed by us, which can solve the problems of main body qualification, standardization, value-added services and inter-bank online payment existing in our country. In this mode, the transaction data of the whole country through online payment is centralized to the union-bank centre; this will facilitate the implement of some value-added services such as anti-money laundering, anti-tax evasion, and credit evaluation.

(2) The system is distributed. The "head office/ branch" mechanism was used in union-bank mode. Likewise, the AML systems of the head office and branch are in different cities, or in different districts of a city. Each level of system is integrated, and need to process the data of its own on business. At the same time, the data exchange and processing among them are necessary and important too. This requests the using of distributed system. Besides, the money laundering behaviors always can not be confirmed by just one deal, and it's necessary to trace the several layers of the capital resource, so the amount of the data referred is enormous. Especially the AML system we discussed centralizes the transaction data of the whole country through online payment, so the workload is gigantic and can't be finished just by one or several computers. Many computers, even many nets are needed to carry on distributed calculation.

(3) The system is real-time and dynamic. The AML system monitors the real-time data including user and transaction information, stores the data into database and carries on the data mining to analyze the inherent relation, and then export the result to relevant department. The whole process is real-time and dynamic.

(4) The system is based on multi-agent. The AML is a complicated calculating work. All kinds of information about money laundering are fuzzy, and often are hiding within the data which seems to have no connection. It is difficult to mine the inherent relation just by one mean. This system uses the multi-agent technology, and every agent completes its function independently. The system filters the data through each agent one by one, and each agent then judge the transaction behavior by whether the data meet their judging condition or not.

3. OVERALL FRAMEWORK DESIGN

The system has adopted hierarchical structure and multi-agent technology, whose logical frame is shown in Fig 1.

The distributed database layer is used for storing the data information correlated with trading, including user information, transaction information and capital flow information. Besides, we designed a historical database to store the historical information; AML basic data resource layer includes AML data warehouse and relevant knowledge base, case base, money laundering shape model base and shadiness base; Data analysis layer is the core of the whole system. It monitors and analyzes the real-time dynamic transaction information using the multi-agent technology under the guidance of basic data resource layer, and outputs the analysis result feedback; Application layer takes the charge of formatting and filing the data input, and output the

* This item is supported by the National natural science fund item (No. 70572079/G021004).

result from data analysis layer to early warning centre and relevant department; Interface layer is used for receiving information from internet, including information from buyer and seller, each commercial bank, revenue, CIQ, police bureau, prosecutorial office and so on. Besides, the interface layer take the charge of reporting the money laundering behavior to the PRC, national information security centre and other relevant department. If there is an application for transferring the suspicious capital to overseas, the union-centre will apply to the PRC for blocking this capital.

The work procedure of this system is shown below: At first, the application layer will clean up and filter the information from interface, and then store the data into database. Then, when the data flow from database is input to the data analysis layer, the AML real-time dynamic monitoring agent will construct the channels to the basic data resource base layer which will control and drive its action. For example, when the AML real-time dynamic monitoring agent receive the data, it will send a "How to deal with" request to the basic data resource base. The basic data resource base then give a "Transfer case-based reasoning agent" response according to the knowledge structure itself. The AML real-time dynamic monitoring agent will transfer the case-based reasoning agent, and produce an interrupt. When the case-based reasoning agent receive the transferring order, it will response immediately and analyze the data through the case reasoning, find out if there is a matching and bring the matching transaction into the shadiness base, return the remainder non-matching data which is undistinguishable afterwards. The AML real-time dynamic monitoring agent then send the request to basic data resource base again and Keep this operation repeatedly transferring each agent in certain order till the basic data resource base think that it's unnecessary to do any transferring. Finally, the result is input to union-bank centre and the basic data resource base for updating and learning self.

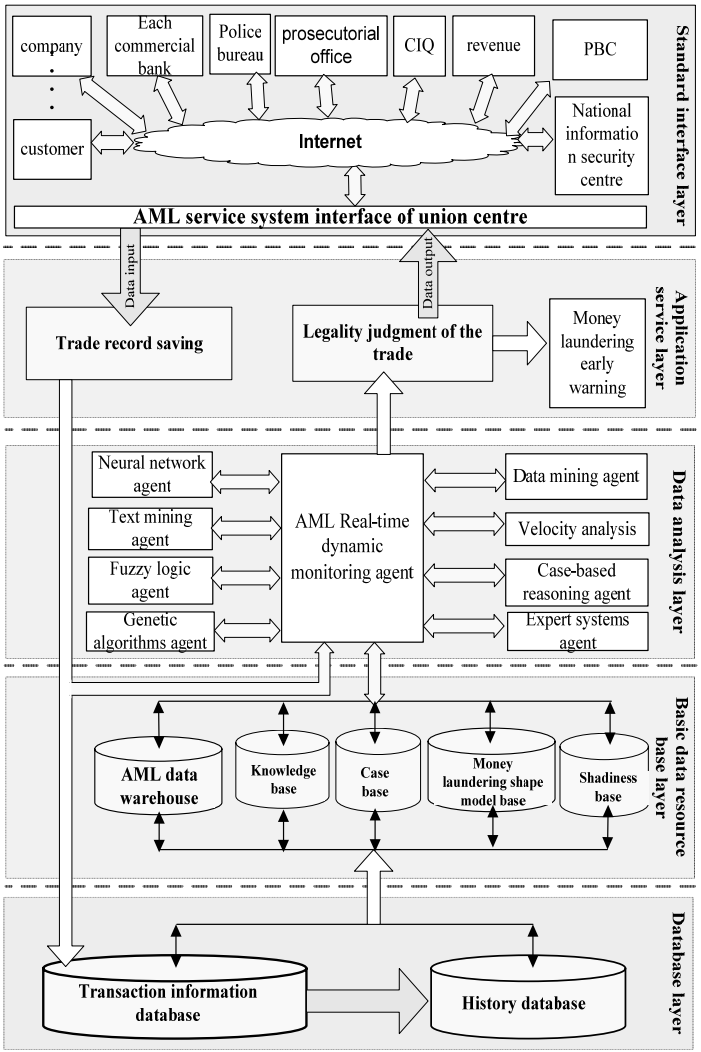


Fig.1. The logical framework of the AML service system

4. KEY AGENT DESIGN

4.1 Data Mining Agent

Data mining is to analyze the data set get by observation (often very huge) whose aim is to find out the unknown relation and summarize the data in a way which the data processor can understand. The data mining agent is one of the most important parts of the AML system, which can excavate out relevant rule from a large amount of data, and enrich the knowledge base and the money laundering shape model base.

4.1.1 Work Principle

The data mining agent of AML system is composed of data resource module, pretreatment module, data mining module, knowledge base module and early warning module. Its structure is shown in Fig 2.

The work procedure of this agent:

(1) Data resource module input data from distributed database layer and data warehouse, and then gives them to the pretreatment module.

(2) Data pretreatment module carries on analysis, and processes the data into record format which can reflect the route of the capital flow.

(3) Data mining module search the relevant rule of money laundering shape model base. If there is a match, the early warning module will send out an alarm. By contraries, if there is no match, the data mining module will store the data using database and data warehouse technologies, and then construct the index.

(4) Classify and clustering process the data in the database so as to facilitate the operation of fast search and data mining. Then carry on the data search and relation mining.

(5) Evaluate the result of searching and mining, store the knowledge expression way which the users can discern into the knowledge base.

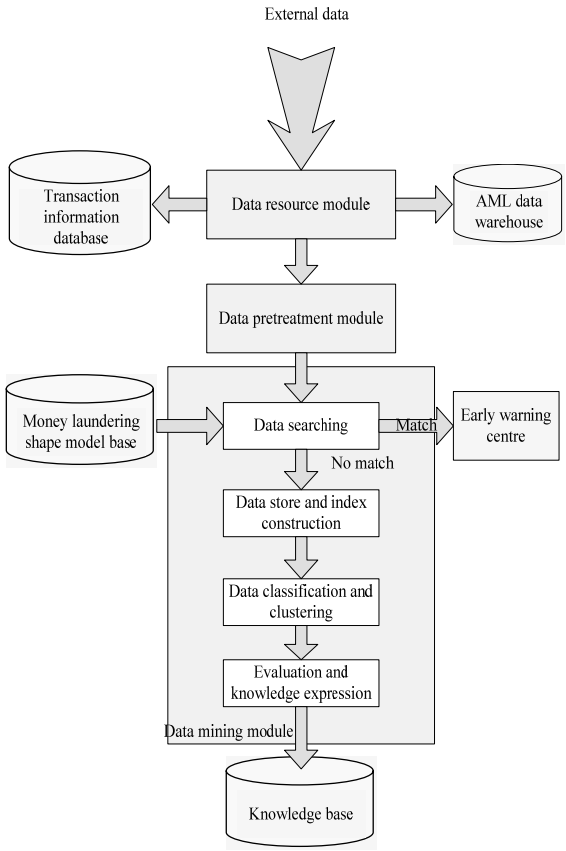


Fig.2. Structure procedure of data mining agent

4.1.2 Key Algorithm

Classify: mapping a data set into several classes which have been defined. The output result of this kind of algorithm is the classifier, and usually is expressed as decision tree or rules set.

Relation analysis: analyze the relation among the data record in the database, utilize the pertinence among the system attribution of the audit data as the basis of constructing normal using mode. The algorithm is described as follows:

Suppose i is the set of items; data D, which relates to the task, is the set of database transactions, among them each transaction is the set of items, each of A and B is one item set. Relation rules are implications like A=>B, $A \subset I$, $B \subset I$, and $A \cap B = \varphi$. Rule A=>B is tenable in transaction set D with support s (s= support(A=>B) = $p(A \cup B)$) and confidence c (c = confidence(A=>B) = $p(B \cup A)$). The s is the percentage of the area which includes $A \cup B$ within the transactions in D, and the c is the percentage of the area which includes A and B within the transactions in D. The rules which meet both the threshold values of can be named as high relation rule. If the item set meet the minimum support, it can be called frequent item set. The process of relation rule mining should be realized by two steps: (1) Find out all the frequent item set. The frequencies of appearance of these item set must get the minimum support count predefined at least. (2) Produce high relation rule by frequent item set. These rules must meet minimum support and minimum confidence. Introduce relation rule mining technology based on constraint to the early warning system. By the mining based on constraint, users can illuminate the data they want to mine according to the aim they are concerned about. So the efficiency of the mining process can be improved.

Sequence analysis: Obtain the sequence mode model. This kind of algorithm can find out the time sequences occurring frequently in audit events. These frequent event modes provide guiding criterion for the choice of statistical feature when constructing early warning system model. The algorithm is described as follows:

Suppose D is a known event database, each transaction T in D relates to time-stamp. The transaction begins at time stamp t_1 and is over at time stamp t_2 according to the order of interval $[t_1, t_2]$. For the project set X in D, if some interval includes X, but its proper subinterval doesn't include X, this interval can be called minimum appearance interval of X. The definition of support of X is the amount proportion of minimum appearance interval accounting for the record in D. Its rule is expressed as X, Y->Z, [confidence, support, window]. In this formula, X, Y, and Z are item set in D. The rule support is support $(X \cup Y \cup Z)$ and the confidence is support $(X \cup Y \cup Z)$/support $(X \cup Y)$. The width of each appearance must be smaller than window value.

4.2 Case Based Reasoning Agent

Case Based Reasoning (CBR) is a kind of analogy reasoning method. Its basic idea is that when solving new problem, we can reason utilizing the former experience of solving similar problem. The main procedure includes: description of new problem → similar case searching → scheme adjusting → scheme assessing → case leaning and maintaining. The CBR agent of AML system first visits the case base of basic data resource base layer and judge the current transaction behavior by matching the characteristics of similar case. The design of CBR agent mainly includes three parts that knowledge expression of case, searching method and self-learning of case.

4.2.1 The Knowledge Expression of Case

During the process of CBR of AML system, the knowledge expression of case is the basis of reasoning which will influences the searching, matching, revising and learning of case directly. The expression of one case should include three parts which are description of money laundering information, description of money laundering characteristics and result set. Its frame is shown in form 1.

4.2.2 Searching Method of Case

We use the rough set theory in this paper. Judge if the existent attribution has the same importance in a given classification using existing information; distribute the characteristic weight value for each attribution according to such importance. Then calculate the semblance of the new problem and the resource cases in the case base utilizing semblance formula in similitude theory. Finally search the most similar case according to the semblance sequence. For given knowledge expression system S (U, A, V, F), $A=C \cup D$, the comprehensive weight of certain attribution r can be calculated by following steps:

(1) Collect a large number of history assessment sample, carry on attribution discretization processing of rough set.

(2) Calculate the importance of attribution r in condition attribution according to the formula:

$$U_c(r)=\text{Card}(pos_C(D))-\text{Card}(pos_{c-r}(D))/\text{Card}(u) \quad (1)$$

In this formula, Card () is the set base, pos () is the positive region of set.

(3) Calculate the objective weight of attribution r according to the formula:

$$W_r=U_c(r)/\Sigma U_c(r) \quad (2)$$

(4) Expert give the subjective attribution Q_i (i=1, 2, ... , n) of each attribution in condition attribution set, among them $Q_1+Q_2+...Q_n=1$.

(5) Choose experience factor α according to the interest of the decision maker, calculate the comprehensive weight of attribution r according to the formula:

$$L_r=\alpha Q_i+(1-\alpha)W_r \quad (3)$$

Form 1: Structure frame of money laundering case

Serial number of money laundering case:
Frame name: (name of money laundering case)
Layer 1. Description of money laundering information
Layer 1.1 Money launderer information
Layer 1.2 Amount of money laundered
Layer 1.3 Route of capital flow
Layer 1.4 Description of money laundering event
Layer 2. Description of money laundering characteristics
Layer 2.1 Money laundering index 1 (index 1, value 1, weight 1; index 2, value 2, weight 2 ...)
Layer 2.2 Money laundering index 2 (index 1, value 1, weight 1; index 2, value 2, weight 2 ...)
...
Layer 2.n Money laundering index n (index 1, value 1, weight 1; index 2, value 2, weight 2 ...)
Layer 3. Result set
Layer 3.1 Breakthrough point of distinguishing from this money laundering behavior.
Layer 4. Relevant knowledge about this money laundering event

4.2.3 Self-learning of Case

The self-learning of case is divided into success learning and failure learning. The success learning refers to two meaning: one is reasoning success; the other is case base learning, namely the increase of new case. Concretely, reasoning success is that the similar case in data base can be regarded as the judging basis and solution of the problem case after adjusting and revising. Case base learning is that if there is some case in case base whose semblance is greater than the given threshold value a (i.e. a=90%), the problem case doesn't join case base. Otherwise the problem case joins case base as new case. Likewise, the failure learning refers to reasoning failure learning and case base learning too.

4.3 Neural Network Agent

In numerous artificial neural network models, the Self-Organizing Map (SOM) is used extensively because of its peculiar brain imitation learning behavior. The "learning without a teacher" phenomenon of brain nerve can be imitated vividly by self learning function of SOM. The cell clustering function of brain nerve can be reproduced accurately by the fair competition mechanism of SOM too. Applying this characteristic to AML area, we can judge the legality of the transaction behavior effectively according to the information hiding in huge fuzzy unordered data, and improve the capability to distinguish money laundering behavior a lot. However, the AML system which centralizes the transaction data of whole country involves a lot of data needed to be traced, and every layer of route of every sum of money refers to many resources, so the computational complexity is huge. We suggest adopting the parallel SOM algorithm. Utilizing the parallel process characteristic of the quanta calculation, atom can deal with 2L numbers using L Qubits at the same time, and complete the calculation of 2L numbers of computer within one step.

Suppose the input vector signal x' = (x(1), x(2), ... , x(M)). If the data learned can be divided into P classes, the amount of nerve cell of SOM input layer is MxP. Define X = (x1, x2... xP) MxP, here, x =x1 = x2...= xP. The amount of nerve cell of SOM output layer is MxP too; Define output nerve cell matrix Y, and its elements are y(i, k), i = 1, 2, ... M, k = 1, 2, ... , P. There is only one connection between each input nerve cell xk(i) and output nerve cell y(i, k). The weight in the t times update is wt(i, k), (Wt, i = 1, 2, ... M, k = 1, 2, ... , P , t = 1, 2, ... ,T). Here, t is the times of update which equals learning/training times of SOM. The concrete algorithm is shown below:

(1) One-off learning: input the all the data need to be learned to the network: x' = (x(1), x(2), ... , x(M)). P*x is X parallel input system.

(2) Weight initialization. Choose random initial value of weight: $w_0(i, k)$. Each initial weight element is unequal and slightly smaller than the input data on the order of magnitude.

(3) Competition process: Repeat the 3, 4, 5, 6 steps of t times; Assign $W_t = V$, here V is the temporary conversion matrix. In the first step of the algorithm, $W_1 = W_0$. Calculate all the Euclidean distance $d_t(i, k)$, i = 1, 2 ... M; k = 1, 2 ..., P, then we can get the distance matrix:

$$D_t=\| X-W_t \| \quad (4)$$

Calculate the minimum using Euclidean minimum distance criterion:

$$d_t(i, k_{min}) = \min(d_t(i, 1), d_t(i, 2), ... d_t(i, P)); \quad (i = 1,2,...,M) \quad (5)$$

(4) Weight update: According the order of i, update the weight utilizing the formula below:

$$w_{t+1}(i, k_{min}) = w_t(i, k_{min}) + \eta(t)[x(i)-w_t(i, k_{min})], \quad k= k_{min}$$
$$w_{t+1}(i, k) = w_t(i, k) \quad (6)$$

Here, η(t) is learning speed constant, k_{min} is the winner of the competition (k = 1,2, ...,P). The η (t) change as the weight update times t. Its common change rule is $\eta(t)=\eta_o[1.0-t/T]$,here ηo is the initial value of η(t).

(5) Suspension condition: There are many conditions for suspend weight update, among them the most popular condition is weight convergence precision control. For a given precision matrix ε, its factor ε(i, k)=ε is a given function which is small definitely. If the condition that $W_{t+1}-W_t < \varepsilon$ can not be satisfied, continue the next step, otherwise turn to step 7.

(6) Weight conversion: In order to obtain the influences of each input data to weight matrix wt and avid the

appearance of part minimum phenomenon during the update process, the weight conversion matrix Q is introduced, QQ－1=I. Its function is reorganizing the element distribution order of the weight matrix.

(7) Weight store: If the condition of Eq. (4) can be satisfied after update, store the weight matrix and stop the calculation process.

4.4 Genetic Algorithm Agent

Genetic algorithm is a kind of searching optimization algorithm based on genetics. The Genetic algorithm agent uses it to analyze the data in the shadiness base, and mine the potential new attribution which will help to find out money laundering behavior. And add it into knowledge base as new identification method.

Genetics think heredity is a way encapsulating the instruction code into each chromosome as gene. Each gene has special position in chromosome and controls certain special attribution. The individual composed of genes has certain adaptability to the environment. Gene hybridization and gene mutation can produce the later generation who has stronger adaptability to the environment. By the natural selection which select the superior and eliminate the inferior, the gene with high adaptability will be kept. This characteristic can be well used in AML area for identifying money laundering behavior. The genetic algorithm agent analyzes the input data, find out the data with most adaptability to the money laundering condition.

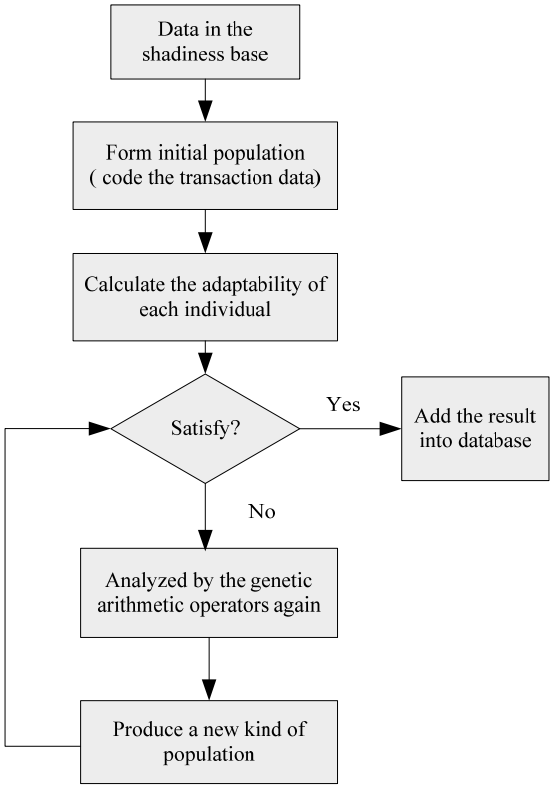


Fig.3. Procedure of genetic algorithm agent

There are two necessary data conversion operations in the genetic algorithm: one is Coding, the other is Decoding. Coding is the process of converting the parameter in the searching space into chromosome individual in the hereditary space while decoding is the inverse operation. The genetic algorithm is a kind of colony operation which regards all the individuals in the colony as object. The three main arithmetic operators that Selecting, Crossover and Mutation make up of Genetic Operation and endow the genetic algorithm with the particular characteristics. The process procedure is shown in Fig 3.

The solution after coding is called chromosome. Choose N chromosomes to construct the initial population at random, and then calculate the adaptability of each chromosome according to predefined evaluating function. Duplicate the chromosomes with good adaptability. By the three arithmetic operators of selecting, crossover and mutation produce the new generation of chromosome with higher adaptability and form new population. Through constant duplication and evolvement generation by generation, the characteristic be converged into an individual with the most adaptability, which is the solution of the problem.

5. CONCLUSIONS AND EXPECTATION

The distributed heterogeneous AML system is designed as one of value added service of the union-bank centre, which improves the ability of identifying the money laundering behavior. The subsystems setting in the transaction system on each level work independently but are interrelated. In this paper, we constructed the structure frame of the AML system based on multi-agent, and designed the key agent. The key to improve the efficiency of this system is the input data. The more abundant and concrete the input data is, the higher this system work. So we suggest use such AML monitoring system in the union-bank online payment mode which centralizes the data of online transaction of the whole country. Thus the popularization of the union-bank mode has a great influence on the AML system we discussed. We expect the union-bank mode we proposed will become the lead online payment mode in the future, and provide a good platform for the AML system. Our next step work is to study deeply on the concrete realization of each agent, and carry on further study on the union-bank mode to supply better environment of the AML work.

REFERENCES

[1] Wang Min, Gao Zhendong, “Study on Financial Risk Early Warning System based on CBR”, in *GROUP ECONOMY*, Nov 2006, No.212, pp.171.

[2] Zhang Chenghu, Li Shi, “Design of Anti-Money Laundering System based on AI technology”, in *Financial Computer of China*, 2005, No.3, pp.44-47.

[3] Yang Yufeng, “The Network Virus Precaution System Based on Data Mining”,in *Journal of Shaoguan University*, Vol.26,Dec.2005,No.12,pp.31-33.

[4] Cheng Yunkai, Lu Zhengding, Li Ruixuan, Li Yuhua, “Anti-Money Laundering System Architecture under Distributed Heterogeneous Environment”, in *Computer Engineering and Applications*,2005,No.29,pp.202-204.

[5] Li Wei Gang, “Algorithm and Characteristic of Parallel Self Organizing Map”, in *China Computer World*,1998, No.49

Qifeng Yang is an Associate Professor, syndic of Hubei e-commerce institute, expert of e-government and e-commerce in development and reform commission of Hubei and dean of e-commerce in economic college, Wuhan University of Technology. He got the master degree from Hua Zhong University of Science and technology in 1993, and doctor degree from Wuhan University of Technology in 2006. He was a senior engineer in head office of China Construction Bank during 1993-2002, and took part in more than 10 large-scale project of computer application software development, and got 1 first prize, 2 second prize of Science & Technology progress in head office of CCB, and 1 second prize of Science & Technology progress in PBC. Now he takes part in one project of National Natural Science foundation as main member, and takes charge several ministerial projects. His research interests are in network finance & e-payment, knowledge management, business intelligence, e-commerce and e-government.

A Hierachical Trust Computation Model for Dynamic Systems *

Yajun Guo, Huiting Wu, Huifang Yan
Department of Computer Science, Huazhong Normal University
Wuhan, Hubei 430079, China
Email: ccnugyj@126.com

ABSTRACT

All security services are based on the premise that systems are trustworthy. There doesn't exist an aforehand trust relationship among entities in dynamic systems. To secure transaction, trust relationship must establish in entities. Presently all trust models are flat, which they can not embody well the dynamic characteristic of trust and do not take on well-operability. In this paper, a hierachical trust computation model for dynamic systems is presented. Trust in this model is composed of basic trust and dynamic trust. Basic trust depends on the attributes of an entity, or recommendation the third party, or experience, while dynamic trust relies on application context. This trust structure can explain well the dynamic characteristic of trust and the initial trust relationship between strangers. The application of this trust model shows that it is well-operability.

Keywords: Trust, Trust Model, Dynamic System

1. INTRODUCTION

Dynamic environment is changeable and unpredictable, so security problems in such environment are very different from those in the traditional system, such as (1) the environment is not familiar to the user, and there doesn't exist trust relationship between the user and the owner of the environment; (2) data is usually generated dynamically; (3) user's access right changes dynamically. There must have enough high level trust to interact between principals who don't know each other. The condition of the traditional centralized security mechanisms and the close distributed security mechanism are that there is trust relationship in advance, so security problems for dynamic systems can't be solved well. Presently, there are a lot of researches on the trust model. However, these models are flat, and they can not work well in the dynamic environment. In this paper, we present a hierachical trust computation model in which trust comprises basic trust and dynamic trust. Dynamic trust depends on basic trust. Some key techniques are discussed such as how to form trust, what trust parameters are included and how to evaluate these parameters, how to calculate combination trust level, how to denote trust, how to compare two trust values and so on.

2. TRUST FORMATION

In the daily life, the trust usually correlates with the party's honest, reliability, ability and so on. Generally speaking, a principal trusts another principal means the ability of the principal to complete a specific action or provide a specific service.

Definition 1 (Trust): The trust is the evaluation of the credible, reliable and the security ability in a specific context and the special time.

This definition emphasizes the evaluation of ability about one principal to another principal. The evaluation result may instruct the act of the principal further. The principal is an entity which can participate in interaction. It may be the human, and also may be the software, the hardware or the organization. The context is the information about position, environment attribute (such as noise rank, light intensity, temperature and so on),people, equipment, object as well as software proxy and so on. The context also includes the virtual ability of the system, the activity which the people or the computer entity participate in and the duty which they complete, as well as their environment role, belief and intention.

A principal's experience may affect the trust decision. There exists the direct relation between the experience and the trust.

Definition 2 (experience): The experience of the trusting principal to the trusted principal is an accumulation measure of observations for the interaction result in a specific context and a concrete time stage.

The different application context has the different trust.

Definition 3 (context trust): The context trust is the trust evaluation of principals in a special context. The context trust is only decided by the context.

If principals don't know each other, and there also have no other principals' recommendation, then how to establish the initial trust of the principals? Usually, the trust is related with attributes. Some attributes of principal may manifest some abilities of principal, for example if the principal has the driver license, then it indicates that the principal has the ability to drive. If the principal has the bachelor diploma for the computer department, then it indicates that the principal has the ability to operate computer.

Definition 4 (attribute trust): The attribute trust is the evaluation of the credibility, reliability and security ability of the trusted principal according to the attributes of the trusted principal.

3. TRUST EXPRESSION

A key question of designing trust model is how to express the trust. The trust expression may be qualitative, and also may be the quantitative. The quantitative trust expression is indicated with a continual real value, and it has an upper boundary and a down boundary. The qualitative expression is usually indicated by using "trust", "untrust" and so on.

In this paper, the trust is discretely expressed as *untrust, uncertainty, low, medium, high*. Here the trust value "*uncertainty*" has several meanings: It may be uncertain in common sense, and also may be uncertain about whether the trust value of the principal is *medium* or *high*. The relationship among these trust values is illustrated in figure 1. @ expresses the complete *uncertainty*, Δ expresses the uncertainty about whether the trust value is *low, medium,* or *high*, and * expresses the uncertainty about whether the trust value is *high*, or *low.*

* Supported by National Natural Science Fundation of China (60403027); Natural Science Fundation of Hubei Province of China(2005ABA243).

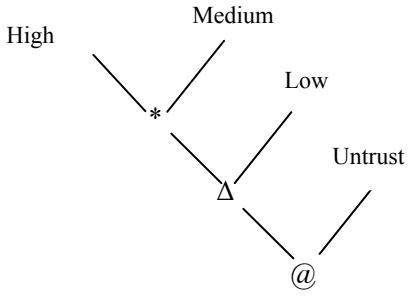


Fig.1. The relationship among trust values

Theorem 1: The relationship among trust values is a partial ordering.

Definition 5: It is supposed that A is the set of the trust values, $\forall a, b \in A$, a≤b or b≤a .

Definition 6 (Structured trust model): A trust model represents the trustworthiness of a principal to another principal. Each principal associates a trust value with other principal. The trust value can be expressed as $T = (T_a, T_c)$. Where T_a is the combination trust value and T_c is the context trust value.

T_a and T_c are discretely expressed as {*high*、*medium*、*、*Δ*、*low*、*@、*untrust*}. For example, trust value (*low*，*medium*) expresses that the combination trust value is *low*, and the context trust value is *medium*.

The definition of trust model has expressed the dynamic characteristic of the trust. For example, when a service is requested, the service provider evaluates the principal's trust value T_a. If access control policy is satisfied, this principal is assigned a set of roles. The activation of roles is based on the context trust value T_c. In the different context environment, the context trust value is changeful and the active roles aren't the same, so the service isn't the same.

The trust value usually needs to be compared in practice, so comparable methods of this trust value are given as follows.

Definition 7: $(t_{a1}, t_{c1}) \leq_3 (t_{a2}, t_{c2})$ if and only if $t_{a1} \leq_1 t_{a2}, t_{c1} \leq_2 t_{c2}$

Theorem 2: If $<T_a; \leq_1>$ and $<T_c; \leq_2>$ are partial ordering sets, then $<T_a \times T_c; \leq_3>$ is also a partial ordering set.

Therefore If $(t_{a1}, t_{c1}) \leq_3 (t_{a2}, t_{c2})$, then the trust value (t_{a1}, t_{c1}) is less than the trust value (t_{a2}, t_{c2}) . Example: $\Delta \leq_1 medium$, $untrust \leq_2 low$, then (Δ, *untrust*)$\leq_3$(*medium*，*low*), namely , the trust value(Δ，*untrust*) is less than the trust value (*medium*，*low*)。

4. TRUST EVALUATION

4.1. Experience Evaluation

Experience usually associates with events. Experience value is possibly reduced or increased by an event. Positive trust events can increase the experience value, and negative trust events will reduce the experience. It is supposed that M positive trust events and N negative trust events are occurred in the specific context and the specific time, then the total number of events is $E=M \cup N$. Because the importance of events is different, each event is assigned a weight. The larger the weight is, the more important the event is. An empirical value T_e can be expressed by using a step function, just as figure 2 shows.

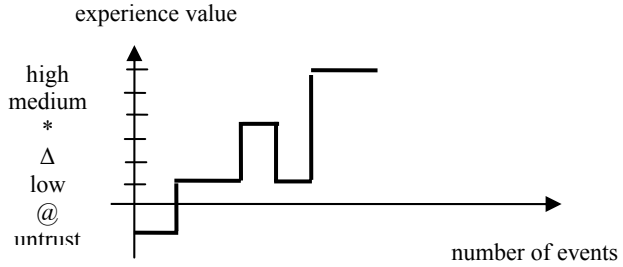


Fig.2. The relationship between the experience and the event

Experience evaluation strategy provides the evaluation method for the occurred event.

(1) Fair strategy

The fair strategy is calculating its experience value according to the number of occurred events completely. Because the experience value is discrete level, the weights may be expressed as 1/15, 1/10, 1/2, 1 and so on. For example, when the positive trust event weight is 1/15, it indicates that 15 positive trust events are needed to increases an experience value level. Opposite when the negative trust event weight is 1/15, it indicates that 15 negative trust events are needed to reduce an experience value level. The change of the total experience value is calculated from the positive or the negative trust event completely.

(2) Optimistic strategy

The optimistic strategy is selecting the positive trust event whose weight is the most in the occurred event to calculate the experience value. For example, there exist some positive trust events whose weights are respectively 1/15, 1/10, 1/2, 1. The optimistic strategy is selecting the positive trust event whose weight is 1 regardless of the negative trust event, so the experience value can increases a level.

(3) Pessimistic strategy

The pessimistic strategy is selecting the negative trust event whose weight is the most in the occurred event to calculate the experience value. For example, there exists some negative trust events whose weights are respectively 1/15, 1/10, 1/2, 1. The pessimistic strategy is selecting the negative trust event whose weight is 1 regardless of the positive trust event, so the experience value reduces a level.

(4) Penalty strategy

The penalty strategy is that the weight of the negative trust event is more than that of the positive trust event to the same event.

4.2 Attributes Trust Evaluation

Automated trust negotiation can establish trust relationship between strangers by disclosing iteratively credentials that include some attributes.

If the access policy of the resource *R* is that the trust value is more than or equal to *medium*, then the trust strategy whose trust value is *medium* may be expressed as: $P \leftarrow B(A_1, \cdots A_K)$. Among them, $B(A_1, \cdots A_K)$ is the Boolean expression of the attribute $A_1, \cdots A_K$. A_i is satisfied, if and only if the other party has exhibited A_i. If $P \leftarrow true$, then the attribute trust value is *medium*. If $P \leftarrow false$, then the attribute trust value is smaller than *medium*. Therefore the attribute trust value is the attribute function of the trusted principal: $T_a^{'} = f(A)$. A is the attributes of the trusted principal.

4.3 Context Trust Evaluation

Trust strategy is different in the different application context. For example, the trust strategy of a printer may be *medium* when the printer is free and the principal is in the office. And may be *low* when the principal is not in the office, or when the printer is busy. The context trust value is the function of the context information: $T_c = h(C)$. C is the context information.

4.4 Recommendation Trust Evaluation

In order to calculate the recommendation trust combination value conveniently, the trust graph of the principal is used here. Each principal saves a trust graph of trust relationship with the other principals.

Definition 8 (trust graph): The trust graph is a unidirectional trust relationship graph between principals: $G = (V, E)$. V expresses the principal, $E = V \times V$ expresses the trust relationship among principals, and $<v_1, v_2>$ expresses that v_1 trusts v_2.

Definition 9 (trust path): A trust path from principal P_i to P_j is expressed that there exists a trust principals sequence $P_{i+1},...,P_n, ..., P_{j-1}$ between P_i and P_j, where P_i trusts P_{i+1}, P_{i+1} trusts P_{i+2}, … , and P_{j-1} trusts P_j.

It is supposed that the trust graph of the principal A have $P_1,...,P_k$ paths to the principal B. There are a set of recommenders $C(P_i) = \{R_{i1},R_{i2},...,R_{in}\}$ on the ith path.

Definition 10: The path of $P_1,...,P_k$ are not related, if exist:

$$\forall P_i, P_j, \forall C(P_i) \cap C(P_j) \equiv \Phi, 1 \le i, j \le k$$

Definition 11: The path of $P_1,...,P_k$ are related, if exist:

$$\exists P_i, P_j, \exists C(P_i) \cap C(P_j) \neq \Phi, 1 \le i, j \le k$$

In the trust graph, the trust value of each trust path is

$$T_r = \min\{T_{A1}, T_{12}, T_{23}, \cdots, T_{nB}\}$$

Where T_{A1} expresses the trust value assigned to the first recommender by principal A, and T_{12} expresses the trust value assigned to the next recommender by the first recommender.

(1) If there have k paths which are not related, the combination trust value can be calculated as:

$$T_f = [\frac{1}{k}\sum_{i=1}^{k} T_{ri}]$$

Where [ ] expresses rounding down to the nearest integer. In order to calculate conveniently, the discrete trust value *high*、*medium*、*、*low*、@、*untrust* can be replaced by using number 7、6、5、4、3、2、1 respectively. So （*high* + *medium*）/2 is replaced by（7+6）/2 =6.5 which is rounded down to the nearest integer as 6, namely, the trust value is *medium*. If different path has different recommendation effect, then the weight is defined as $\omega_i (\omega_i \ge 0, \ and \ \sum_i \omega_i = 1)$. The combination trust value can be calculated as:

$$T_f = [\sum_{i=1}^{k} \omega_i \times T_{ri}]$$

(2) When there are k paths which are related, in which m paths aren't related ($m < k$), the combination trust value can be calculated as:

$$T_f = [\frac{1}{m}\sum_{i=1}^{m} T_{ri}]$$

If different recommendation path has different recommendation effect, then the weight is defined as $\omega_i (\omega_i \ge 0, \ and \ \sum_i \omega_i = 1)$, so the combination trust value can be calculated as:

$$T_f = [\sum_{i=1}^{k} \omega_i \times T_{ri}]$$

5. TRUST MODEL APPLICATION

In this part, we illustrate a dynamic authorization by combining trust model and role-based access control (RBAC) model. When a principal requests to obtain a service, it is supposed that security policy of this service is that trust value must be more than or be equal to T_n. Access control operations are as follows:

(1) The principal's trust value Ta is calculated.
(2) If Ta is less than trust value Tn, then turn to (3);
(3) The service provider requests to make trust negotiation with the principal until the attribute trust value equal to the value Tn. If the negotiation fails, then the access fails;
(4) The principal is assigned a role set.
(5) The service provider evaluates the context trust value Tc, the different context trust value will activate different roles. Therefore the principal obtains the different service.
(6) If the context trust value is less than the activation role's trust value, then the access fails.
(7) So the access control model based on the trust model is composed of following several parts:

- *Users*、*Roles*、*Perms*、*T* and *Sessions* respectively denote the set of users, roles, permissions, trust values and sessions. The meaning of T_a and T_c are the same as the introduction above.
  The relations *UA, TA, PA* define the associations of user-trust _value assignment, trust _value –role assignment, and permission-role assignment.
- $UA \subseteq Users \times T$, a one-to-many mapping of user-to-trust _value assignment relation. A user is assigned a trust value, and a trust value may be assigned to many users.
- $TA \subseteq T_a \times Roles$, a many-to-many mapping of trust _value-to-role assignment relation.
- $PA \subseteq Perms \times Roles$, a many-to-many mapping of permission-to-role assignment relation.
  Trust values assignment, roles assignment and permissions assignment are defined in the following functions:
- *Assigned_trustvalue (t : T)* = $\{u \in Users \mid (u,t) \in UA\}$ expresses trust value t to a group of users' mappings.
- *Assigned_roles (u: Users, t: T_a)* $\rightarrow 2^{Roles}$ returns the role set of the assigned users.
- *Assigned_permissions (r: Roles, t: T_c)* $\rightarrow 2^{Perms}$ returns the right set of the assigned role.
  TT, RR and *PP* respectively define the relationship of the trust inheritance, the role inheritance and the permission inheritance:
- $TT \subseteq T \times T$ expresses the dual relationship between the trust value and the trust value. The partial ordering relationship between the trust value and the trust value is formed through inheritance relationship, which is expressed as $\ge$. $t_1 \ge t_2$ expresses that trust value t_1 has all roles of t_2.
- $RR \subseteq Roles \times Roles$ expresses the dual relationship between the role and the role. The partial ordering relationship between the role and the role is formed through inheritance relationship, which is

expressed as ≥. $r_1 \geq r_2$ expresses role r_1 has all rights of r_2.

- $PP \subseteq Perms \times Perms$ expresses the dual relationship between permission and permission. The partial ordering relationship between permission and the permission is formed through inheritance relationship, which is expressed as ≥. $p_1 \geq p_2$ expresses p_1 has all permissions of p_2, and all roles of p_1 are also roles of p_2.

REFERENCES

[1] L. J. Hoffman, K. Lawson-Jenkins, J. Blum, "Trust Beyond Security: An Expanded Trust Model," *Communications of the ACM,* Vol.49, No.7, pp.94-101, 2006

[2] Y. L. Sun, W. Yu et al, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications, Vol.24, No.2*, pp. 305-317, 2006.

[3] A. A. Pirzada, C. McDonald, A. Datta, "Performance Comparison of Trust-Based Reactive Routing Protocols," *IEEE Transactions on Mobile Computing*, Vol. 5, No.6, pp. 695-710, 2006.

[4] M. Carbone, M. Nielsen, V. Sassone, "A Formal Model for Trust in Dynamic Networks," *in Proceedings International Conference on Software Engineering and Formal Methods*, pp. 54-61, 2003.

[5] S. Song, K. Hwang et al, Trusted P2P Transactions with Fuzzy Reputation Aggregation," *IEEE Internet Computing*, Vol.9, No.6, pp.24-34, 2005.

[6] A. Jøsang, S. Pope, "Semantic Constraints for Trust Transitivity," *in Proceedings of the 2nd Asia-Pacific conference on Conceptual modeling, Newcastle*, *Australia*, pp. 59-68, 2005.

[7] H. Li, M. Singhal, "Trust Management in Distributed Systems," *Computer*, Vol.40, No.2, pp.45-53, 2007

[8] N. Li, J. C. Mitchell et al, "Beyond Proof-of-Compliance: Security Analysis in Trust Management," *Journal of the ACM*, Vol.52, No.3, pp.474-514, 2005.

Self-certified Digital Signature Scheme in Manufacturing Grid Environment*

Youan Xiao
School of Information Engineering, Wuhan University of Technology
Wuhan, Hubei Province 430070, P. R. China
Email: youan@21cn.com

ABSTRACT

Self-certified digital signature is an important information security technology for the manufacturing grid environment. In this paper, a new self-certified digital signature scheme based on the elliptic curve discrete logarithm problem is proposed. It has the ability to solve the performance problems in the certificate authority, overcome the disadvantages of the known digital signature schemes. Furthermore, we also analyzed the new scheme's computational complexity and security. The new scheme, which is an extension of elliptic curve cryptosystems, is beneficial for the study on the domain for the self-certified digital signature. It is quite suitable for the environment of manufacturing grid.

Keywords: Manufacturing Grid, Digital Signature, Self-Certified Digital Signature, Elliptic Curve

1. INTRODUCTION

To face the rapid advancement of network technology and distributed computing, the manufacturing enterprises must adapt themselves to this trend by changing their manufacture mode. The globalization has been one of the most pervasive and promising business model in manufacturing process in order to implement the cost-effective and efficient production management among the manufacturing enterprises which geographically located anywhere in the world. However, the lack of effective mechanisms to support real collaborations such as collaborative working and manufacturing resource sharing among manufacturing enterprises prevents all the collaborators from realizing the maximum value of the fanned engineering and service chain[1]. Manufacturing grid faces the development requirements of the manufacture technology, and tries to applies the grid technology to the manufacturing industry in order to realize resource sharing and collaborative working among distributed manufacturing enterprises and different departments of one enterprise based on the Internet. It has been one of the most important research direction in the domain of manufacture scientific during the information ear [2].

However, like the Internet, the information security problem is still one of the major remaining obstacles to the wide spread adoption of manufacturing grid [3]. The known grid security infrastructure is based on the public key cryptosystem. In the manufacturing grid system, each user has a pair of keys, one is called as private key which is secret and the other one named as public key which is published in public. There is an institution called as Certificate Authority (CA) which can issue an identity certificate for every public key in order to ensure the authenticity of the published public keys with a user's ID. Any user can sign a message with his owner private key so that any other user can verify whether this signature is valid or not by the public key of the subscriber which can be found in a public directory and can be validated relied on CA. The verifying procedure is based on the following input: the subscriber's public key, his ID, his certificate, the CA's public key and the CA's digital signature.

Compared with other system, the manufacturing grid consists of a collection of heterogeneous resource across multiple administrative domains with the intent of providing enterprises to realize resource sharing and collaboration. It has many distinctive characteristics such as the openness, the dynamic, the autonomy, the isomerism, the huge numerous user population, the dynamic organization member and the great deal of resource pool, etc. So the different mechanisms and frequent processes are required for the authentication and authorization to the grid users and resources in the manufacture grid environment. Therefore, the CAs in the manufacturing grid system suffer from the performance problems in the authentication procedures.

To solve these problems, the concept of self-certified public key was first introduced by Girault[4] in 1998. In the self-certified public key cryptosystem, the public key of each user is generated by the CA from his identity such as the complete name, an email address or an IP address, while the corresponding private key which is only known by the user can be computed from the public key. In this way, the identity certificates are not needed because the authenticity of public keys can be verified implicitly without the CA's digital signature. That is say, the verification of the public keys can be carried out in the signature verification phase of verifying a message's digital signature simultaneously.

The known self-certified digital signature schemes are all based on the integer factor cryptosystem[5] or discrete logarithm cryptosystem[6]. However, these cryptosystems have several fatal flaws such as slower working speed, complex parameters, and longer key. Therefore these self-certified digital signature schemes are unsuitable for the environment of manufacturing grid.

Elliptic Curve Cryptosystem was first introduced by Neal Koblitz[7] and Victor Miller[8] in 1986 independently, which is a kind of public key cryptosystem based on the elliptic curve discrete logarithmic problems (ECDLP). This cryptosystem has relatively shorter key length, lower bandwidth requirements for data, and faster encryption and decryption process when compared with other public key cryptosystems with the same security level[9]. So it is quite suitable for the self-certified digital signature schemes in the environment of manufacturing grid.

In this paper, we proposed a new self-certified digital signature scheme in grid environment based on the elliptic curve cryptosystem. In the proposed scheme, the recipient or verifier can eliminate the burden of verifying the public key before using it with the same workload in digital signature generation phase. This proposed scheme has several more advantages such as shorter key length, lower bandwidth requirements for data, faster working speed, simple parameters,

* This work was supported by the Sunshine Young Project in Wuhan City of China under Grant No.20055003059-5.

and higher security level than the known ones. It has overcome the disadvantages of the known digital signature schemes, and is quite suitable for the environment of manufacturing grid.

The rest of this paper is organized as follows: In section 2, a self-certified digital signature scheme in grid environment is proposed. Section 3 analyzes the proposed scheme. Finally, in Section 4, we draw the conclusion and propose future research.

2. SELF-CERTIFIED DIGITAL SIGNATURE SCHEME

The proposed self-certified digital signature scheme is based on the discrete logarithm problem over elliptic curve groups. For more background information on the elliptic curve cryptosystem, please refer to [9~10]. In this paper, the following parameters and arrangement about the proposed self-certified digital signature scheme over the elliptic curve domain are required:

Supposes E is a security elliptic curve defined over the finite field F_p. The field size p is a large odd prime. Parameter $n = \#E$ is the order of the elliptic curve, which is equal to the number of points on the elliptic curve. G is a randomly selected element of the elliptic curve E called as the base point, whose order r is a large prime divisor of n.

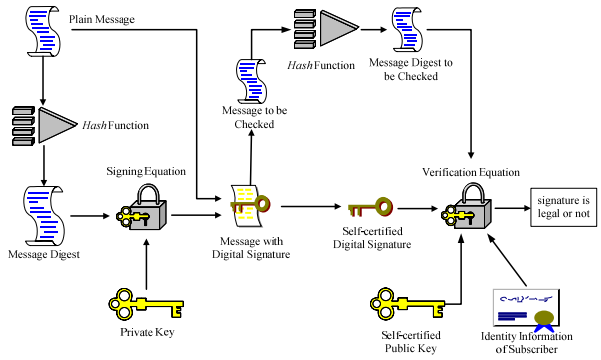


Fig.1. Workflow of self-certified digital signature scheme

Fig.1 shows the workflow of the proposed self-certified digital signature scheme. It shows that the structure of the proposed self-certified digital signature scheme can be divided into three phases, including the self-certified public key generation phase, the self-certified digital signature generation phase, and the self-certified digital signature verification phase. The purpose of the self-certified public key generation phase is generating the public key of a user which contains the user's identity information simultaneously and computing the corresponding private key without leaking the private key of the others including the certificate authority. Then at the self-certified digital signature generation phase, the signer can sign the message with his self-certified private key. The function of the self-certified digital signature verification phase is to let anyone who knows the self-certified public key of the subscriber can verify a self-certified digital signature affixed with a message is legal or not.

2.1 Self-Certified Public Key Generation Phase

Supporting the private key SK_{CA} of the certification centre CA is a secret large random integer in the range [1, r - 1]. And the corresponding public key PK_{CA} is a point on E where $PK_{CA} = SK_{CA} \times G$.

In this phase, user A will get a pair of self-certified public key and private key by executing the follow operations with the CA:

Step 1: User A chooses a secret random integer x which is small than r.

Step 2: User A computes $Y = x \times G$, and sends Y to CA in a public channel.

Step 3: CA chooses a new random integer k which is small than r, and computes $PK_A = k \times Y$.

Step 4: CA computes:

$$q = k^{-1} \times (Hash(ID_A) - SK_{CA} \times (PK_A)_x)$$

where ID_A is the identity information of user A such as the complete user name, an email address or an IP address with X.509 format, and $Hash()$ is a public collision resistant hash function such as SHA-1.

Step 5: CA sends (PK_A, q) to user A.

Step 6: User A computes $SK_A = q \times x^{-1}$, and then verifies it with the following equation:

$$(PK_A)_x \times PK_{CA} + SK_A \times PK_A = Hash(ID_A) \times G \quad (1)$$

Now, user A have gotten the self-certified public key and it's corresponding private key. The private key is only known by user A.

2.2 Self-Certified Digital Signature Generation Phase

When the user A wants to sign a message m with his for self-certified public key, he executes the follow signing operations:

Step 1: User A chooses a random large integer k which is small than r, and computes $R = k \times PK_A$.

Step 2: User A computes digital signature s with following signing equation:

$$S = SK_A \times (Hash(m) + R_x) - k \quad (2)$$

Where $Hash()$ is another public collision resistant hash function. Then the self-certified digital signature is $s = (R, S)$.

Step 3: User A affixes the self-certified digital signature s to the special message m, as the entire message $M = (m, s)$.

2.3 Self-Certified Digital Signature Verification Phase

After the recipient B receives the message M, he can verify the self-certified digital signature by executing the follow steps:

Step 1: The recipient B decodes the plain message m, self-certified digital signature (R, S) from the received message M.

Step 2: Recipient B computes $H_a = Hash(ID_A)$ where ID_A is the identity information of subscriber A and $Hash()$ is the same public collision resistant hash function as the one in section 2.1.

Step 3: Recipient B computes $H_m = Hash(m)$ where $Hash()$ is the same public collision resistant hash function as the one in section 2.2.

Step 4: B verifies the self-certified digital signature is legal or not with the following verification equation:

$$H_a \times H_m \times G + H_a \times R_x \times G = R + S \times PK_A + (H_m + R_x) \times (PK_A)_x \times PK_{CA} \quad (3)$$

The self-certified digital signature is legal when the equation (3) can be brought into existence.

3. SCHEME ANALYSES

3.1 Correct Proving

The correct proving of the proposed self-certified digital signature scheme has two parts: first is the correct proving about equation (1), the other one is about equation (3).
The user A uses equation (1) to verifies the self-certified public key and the corresponding private key. It can be proved as follows:

$$\because \quad SK_A = q \times x^{-1}$$
$$= k^{-1} \times (Hash(ID_A) - SK_{CA} \times (PK_A)_x) \times x^{-1}$$
$$= (k \times x)^{-1} \times (Hash(ID_A) - SK_{CA} \times (PK_A)_x)$$
$$\therefore \quad SK_A \times k \times x = Hash(ID_A) - SK_{CA} \times (PK_A)_x$$

So,

$$SK_A \times k \times x + SK_{CA} \times (PK_A)_x = Hash(ID_A)$$

And,

$$Hash(ID_A) \times G = SK_A \times k \times x \times G + SK_{CA} \times (PK_A)_x \times G$$
$$= SK_A \times k \times Y + SK_{CA} \times (PK_A)_x \times G$$
$$= SK_A \times k \times Y + (PK_A)_x \times SK_{CA} \times G$$
$$= SK_A \times PK_A + (PK_A)_x \times PK_{CA}$$

Therefore,

$$(PK_A)_x \times PK_{CA} + SK_A \times PK_A = Hash(ID_A) \times G$$

From here we see that the equation (1) is correct and can verifies self-certified public key pair is right or not.

Recipient B uses equation (3) to verifies the self-certified digital signature. It also can be proved as follows:

From equation(2), we knows:

$$\because \quad S = SK_A \times (H_m + R_x) - k$$
$$S \times G = (SK_A \times (H_m + R_x) - k) \times G$$
$$= (H_m + R_x) \times PK_A - k \times G$$
$$\therefore \quad (H_m + R_x) \times PK_A = (S + k) \times G$$

From equation(1), we knows:

$$\because \quad H_a \times G = (PK_A)_x \times PK_{CA} + SK_A \times PK_A$$
$$SK_A \times PK_A = H_a \times G - (PK_A)_x \times PK_{CA}$$

So,

$$(H_m + R_x) \times (H_a \times G - (PK_A)_x \times PK_{CA})$$
$$= (H_m + R_x) \times SK_A \times PK_A$$
$$= SK_A \times ((H_m + R_x) \times PK_A)$$
$$= SK_A \times (S + k) \times G$$
$$= (S + k) \times PK_A$$
$$= S \times PK_A + k \times PK_A$$
$$= S \times PK_A + R$$

Therefore,

$$H_a \times H_m \times G + H_a \times R_x \times G =$$
$$R + S \times PK_A + (H_m + R_x) \times (PK_A)_x \times PK_{CA}$$

From here we see that the equation (3) is correct and can verifies self-certified digital signature is legal or not.

3.2 Performance Analyses

Because the self-certified public key generation phase occurs rarely, so the time spent in the self-certified public key generation phase has small effect to the use of the new scheme that it can be ignored.

In the self-certified digital signature generation phase, the main operation is computing the self-certified digital signature s by equation (2). So it is clear that the new scheme needs no more extra operations when compared with the ordinary elliptic curve signature schemes[11~12]. Then the workload is equal to the workload of the ordinary elliptic curve digital signature schemes and much less than the known self-certified digital signature schemes based on the integer factor or discrete logarithm cryptosystem.

At the self-certified digital signature verification phase, the main operation is check the self-certified digital signature s by equation (3). When compared with the verification equation in the ordinary elliptic curve digital signature schemes, the equation (3) needs one extra scalar multiplication of elliptic curve point by integers and two extra addition of elliptic curve points because there is a public key verification progress simultaneously. But when compared with the ordinary elliptic curve digital signature schemes, the new proposed scheme needn't the progress to verify the public key of the subscriber is legal or not. So the workload is much less than the ordinary elliptic curve digital signature schemes and the known self-certified digital signature schemes based on the integer factor or discrete logarithm cryptosystem.

In a word, the new proposed self-certified digital signature scheme is faster than the known ordinary elliptic curve digital signature schemes, and have relatively shorter key length, lower bandwidth requirements, and faster signature generation and verification process when compared with other known self-certified digital signature schemes with the same security level. So it is quite suitable for the environment of manufacturing grid.

3.3 Security Considerations

Basically, the security of the proposed self-certified digital signature scheme is based on the difficulty of breaking the one-way hash function and the elliptic curve discrete logarithm problem (ECDLP). That is say, the difficulty for any attackers to forge another self-certified digital signature from the equations (1) to (3) are equivalent to the solution complicated by an one-way hash function and the ECDLP problem at the same time. Its difficulty is even than the ECDLP itself.

There are several security properties such as unforgeability, verifiability, undeniability, identifiabitity, etc. In this section, we shall consider some possible attacks against the proposed scheme. We shall prove that the proposed scheme can withstand these possible attacks.

Attack 1: Someone tries to derive the private key of user A from the available public information about the user A.

Analysis of Attack 1: The public information about the user A includes the public key PK_A and identity information of user A. Assume the adversary wants to derive the private key of user A from the public key PK_A and identity information ID_A. He must solve the SK_A from the equation (1). That is say, he must solve the following equation:

$$SK_A \times PK_A = Hash(ID_A) \times G - (PK_A)_x \times PK_{CA} \quad (4)$$

It's clear that the equation (4) is as difficult as breaking the elliptic curve discrete logarithmic problem. Therefore, it's impossible to obtain the private key of user A from the public information.

Attack 2: Someone tries to derive the private key of user A from a message and its corresponding digital signature.
Analysis of Attack 2: Assume the adversary wants to derive the private key of user A from the message m, its corresponding digital signature s, the public key PK_A and the

identity information ID_A. He must solve the SK_A from the equation (2) and the equation $R = k \times PK_A$ at the same time. Apparently, it is as difficult as breaking the elliptic curve discrete logarithmic problem. The adversary cannot derive the private key of user A from a message and its corresponding digital signature. Therefore, there are none aggressors can forge a valid self-certified digital signature too.

Attack 3: Someone tries to forge a valid self-certified digital signature by deceiving the recipient B.
Analysis of Attack 3: Anyone who wants to forge a valid self-certified digital signature must knows the private key of user A or breaks the public collision resistant hash function. With the security analyses above, it is impossible to obtain the private key of user A. On the other hand, breaking the public collision resistant hash function such as SHA-1 is very difficulty. So there are nobody can forge a valid self-certified digital signature.

Attack 4: User A tries to deny a valid self-certified digital signature after he signed a message.
Analysis of Attack 4: Assume user A wants to deny a valid self-certified digital signature after he signed the corresponding message, he must break the public collision resistant hash function. With the security analyses above, breaking the secure public collision resistant hash function is impossible. Therefore, user A cannot deny a valid self-certified digital signature after he has signed the corresponding message.

Based on the security consideration above, we can get a conclusion that the proposed self-certified digital signature scheme is security.

4. CONCLUSIONS

In this paper, we have proposed a new self-certified digital signature scheme based on the elliptic curve discrete logarithm problem. This scheme is securer and faster than the known ones. In the proposed scheme, the recipient or verifier can eliminate the burden of verifying the public key before using it with the same workload in digital signature generation phase. It has overcome the disadvantages of the known digital signature schemes. Some possible attacks have been considered. None of them can successfully break this proposed scheme. Therefore, the proposed scheme is quite suitable for the environment of manufacturing grid.

REFERENCES

[1] Xiao Youan, "Researches On The Basic Theory And The Key Technique About Information Security In The Manufacturing Grid," Wuhan: Post doctor Research Report for Wuhan University of Technology, 2006.

[2] Qiu, R.G., "Manufacturing grid: a next generation manufacturing model," in *Proceeding of IEEE International Conference on Systems, Man and Cybernetics*, 2004, Vol. 5, Oct. 2004, pp. 4667~4672.

[3] Hongxia Cai, Tao Yu, et al., "Security solution to manufacturing grid usage scenarios," in *Proceeding of IEEE International Symposium on Cluster Computing and the Grid*, 2005, CCGrid 2005, Vol. 2, May 2005, pp. 638~643.

[4] M. Girault, "Self-certified public keys," in *Proceeding of Conference on Information Security and Cryptology*, Vol.10, No.1, Feb. 1998, pp.89~107.

[5] Lee B, Kim K, "Self-certified signature," in *Proceedings of Progress in Cryptology*. Aug 2002:199~214.

[6] Z. Shao, "Cryptographic Systems Using a Self-Certified Public Key Based on Discrete Logarithms," in *IEEE Proceedings of Computer & Digital Techniques*, Vol. 148, No.6, July 2001, pp.233~237.

[7] Koblitz, N., "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol.48, No.1, January 1987, pp. 203~209

[8] Miller, V., "Use of Elliptic Curves in Cryptography," in *Proceeding of Advances in Cryptology*, CRYPTO '85, Lecture Notes in Computer Science, Vol.218, December 1986, Springer-Verlag, pp. 417~426

[9] Xiao Youan, *Study about the Elliptic Curve Crypto-system*, Wuhan: Huazhong University of Science and Technology Press, 2006.

[10] Youan Xiao, Zude Zhou. Layuan Li, "An Elliptic Curve Proxy Signature Scheme," in *Proceeding of International Symposium on Distributed Computing and Applications to Business, Engineering and Science'2006, DCABES' 2006*, October 2006, pp. 1151~1154.

[11] Komathy K., Narayanasamy P., "Strengthening ECDSA Verification Algorithm to be More Suitable to Mobile Networks," in *Proceeding of International Multi-Conference on Computing in the Global Information Technology*, 2006. ICCGI '06, Aug. 2006, pp. 61 ~ 67

[12] Meurice de Dormale, G., Ambroise, R., et al., "Low-Cost Elliptic Curve Digital Signature Coprocessor for Smart Cards," in *Proceeding of International Conference on Application-specific Systems, Architectures and Processors*, 2006. ASAP '06, Sept. 2006, pp. 347 ~ 353.

Youan Xiao is an associate professor and research supervisor in School of Information Engineering, Wuhan University of Technology. He graduated from Huazhong University of Science and Technology in 1996; and received his PhD. degree from Wuhan University of Technology in 2003. His research interests include information security, computer network, manufacture grid, advanced manufacture and e-commence.

Information Security Evaluation of E-Government Systems

Xiaorong Cheng, Mei Li, Huilan Zhao
School of Computer Science and Technology, North China Electric Power University
Baoding, Hebei 071003, China
Email: joyss1@163.com

ABSTRACT

An information security assessment model based on the systems security engineering capability maturity model (SSE-CMM) is proposed according to characteristics and security requirements of e-government systems. Fuzzy comprehensive judgment is also applied to mitigate the uncertainty of threats and weaknesses in e-government systems. To overcome the subjectivity in fuzzy judgment, assessment factors are calculated objectively by the method of entropy weight coefficient. Finally, the study of a case shows the security degree of an e-government network system can be conveniently found out with this method, while efficiently decreasing the computing complexity and influence form human factors.

Keywords: E-government system, Security assessment SSE-CMM, Fuzzy comprehensive judgment, Entropy-weight

1. INTRODUCTION

Electronic government (e-Government) encompasses a wide range of services and is related to a lot of different fields in the whole society. The security risks existing in an e-Government system may not only influence the secure running of the system but also endanger the government and the public society, even the safety of the country. Therefore the security assessment process has become a major force, driving: creation of information security strategies, build of road maps, prioritization of activities, and selection of safeguards [1-3].
The analytical method based on SSE-CMM model and combines the fuzzy comprehensive judgment is practical and applicable for security assessment in network systems [4-6]. However, the weight vectors of assessment factors in the method above are usually to a large extent dependent on personal judgment, knowledge, and gut feeling of the individual specialist. This paper applies the method of entropy-weight coefficient to overcome subjectivity.

2. ASSESSMENT MODEL OF INFORMATION SECURITY IN E-GOVERNMENT

2.1 Content of Assessment Based on SSE-CMM

Reference [6] combines the model of SSE-CMM into information security assessment of e-Government systems and divides the 22 process areas into 3 basic kinds. In this way the hierarchy structure of assessment model is constructed (Fig.1). This paper makes change to the definition of every process area in reference [6]. Table.1 gives the improved assessment items of process areas.

2.2 Fuzzy Comprehensive Judgment Applied in E-government systems

Table 1. Improved assessment items of process areas.

Process Area	Assessment Items
PA02	Assess the influence of the system
PA03	Assess the risk existing
PA04	Assess the threat existing
PA05	Assess the weakness existing
PA01	Manage the secure running of system
PA07	Harmonize the secure surveillance policies
PA08	Surveil the security state of system
PA09	Supply the secure input of system
PA10	Clear and in detail describe security requirement of system
PA06	Construct security ensurence for the system
PA11	Validate the security ensurence for the system
PA12	Ensure the quality of the system
PA13	Manage security configuration
PA14	Manage item risk
PA15	Surveil the technology of the system
PA16	Soundly plan the technology
PA17	Define system engineering processes
PA18	Improve system engineering processes
PA19	Manage the improvement process of system products
PA20	Manage the supporting environment of the system
PA21	Supply the technology and knowledge for continual improvement
PA22	Harmonize with the provider related to systems

2.2.1 Construct Fuzzy Set: Based on the hierarchy structure in Fig.1 the second level assessment factor set is constructed by (1) and (2).

$$U = \{U_1, U_2, \cdots, U_n\} \quad (1)$$

$$U_j = \{U_{j1}, U_{j2}, \ldots U_{jm}\},\ 1 \le j \le n \quad (2)$$

Each element in U is assessment factors set on the third level. Experts will give remarks of the satisfied degree to each assessment factor according to different judge rules. The remarks are divided into several levels to measure the behavior on the rule and the value of the assessment factors. Different judge set can be set up according to different requirements and rules.

Suppose the judge set here is $V = \{V_0, V_1, \ldots, V_l\}$. And $A_j = (a_{j1}, a_{j2}, \ldots, a_{jn})$ is the weight coefficient set of different assessment factors in U_j.

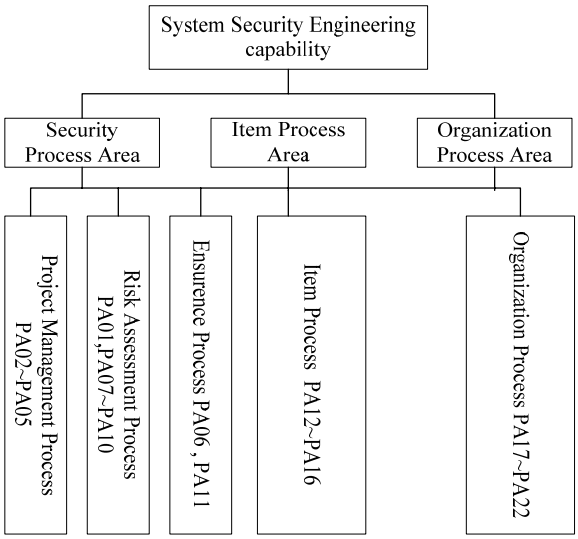


Fig.1. Structure model of information security assessment on E-government systems.

2.2.2 Construct Subjection Degree Matrix R: Experts give remarks to each factor according to different rules; we can construct the fuzzy map f. $f:U\to F(V)$, $U_{ji}\to f(U_{ji})=(r_{i1},r_{i2},\ldots,r_{il})$. It shows the support degree from assessment factor U_{ji} to each remark in judge set. The subjection vector of U_{ji} to the judge set V is denoted by $R_{ji}=\{r_{i1},r_{i2},\ldots,r_{il}\}$, $i=1,2,3,\cdots,m$. The subjection degree matrix R is as follows:

$$R_j=\begin{bmatrix} r_{11} & r_{12} & \ldots & r_{1l} \\ r_{21} & r_{22} & \ldots & r_{2l} \\ \ldots & \ldots & \ldots & \ldots \\ r_{m1} & r_{m2} & \ldots & r_{ml} \end{bmatrix} \quad \textbf{(3)}$$

2.2.3 Construct the Second Level Comprehensive Judgment Model: In order to calculate the security engineering ability of the system, judge matrix on the first level can be set up as follow.

$$H_j=A_j\cdot R_j=(h_{j1},h_{j2},\cdots,h_{jl})$$

$$h_{js}=\sum_{k=1}^{m}a_{jk}r_{ks},1\le s\le n \quad \textbf{(4)}$$

And the judge matrix on the second level is set up as:

$$R=\begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{bmatrix}=\begin{bmatrix} A_1\cdot R_1 \\ A_2\cdot R_2 \\ \vdots \\ A_n\cdot R_n \end{bmatrix}_{l\times n} \quad \textbf{(5)}$$

3. CONFIRM ENTROPY WEIGHT COEFFICIENT OF EACH RISK FACTOR

Traditional methods of calculating weight vectors such as AHP relay heavily on people‘s subjective judgment. This paper applies entropy-weight coefficient method to overcome the subjectivity in calculating weight vectors on the first and the second level.

3.1 Definition of Entropy

The entropy denotes the uncertain degree of the system. Suppose there are n kinds of states of the system: $S_1,S_2,\ldots,S_n$, P_i is the probability of being at state S_i. If anyone in $P_i,i=1,2,\cdots,n$ is known, the entropy can be calculated by $H=-\sum_{i=1}^{n}P_iL_nP_i$, $0\le P_i\le 1$, where $\sum_{i=1}^{n}P_i=1$.

3.2 Extreme of Entropy

According to the extreme of entropy, we know that the nearer P_i reaches, the larger the entropy's value is. If $P_i=\frac{1}{n},(i=1,2,\cdots,n)$, the entropy reaches its maximum $Hmax: H\left(\frac{1}{n},\frac{1}{n},\cdots\frac{1}{n}\right)=L_nn$

3.3 Confirm Entropy-weight Coefficient

For the subjection degree matrix above, the larger the difference of some factor's sustain degree to the index in assessment set, the larger the factor's function in the whole assessment; and if the sustain degrees of some factors are all equal, the results of the experts' assessment would be dispersive, and the assessment are hardly work to the final result.

Based on the extreme of the entropy, we can use entropy to calculate the weight of each factor on the base of the sustain degree r_{ij} of each risk factor to the index in the assessment set.

The method is as follow. The relative importance of the assessment factor can be measured by the following entropy value.

$$H_i=-\sum r_{ij}L_nr_{ij} \quad \textbf{(6)}$$

The nearer r_{ij} reaches, the larger the entropy's value and the larger the uncertainty of the assessment factor to the system's security assessment would be. When the values of r_{ij} are equal, the entropy reaches its maximum which can be used to uniform the equation (6),

$$e_i=-\frac{1}{L_nm}\sum_{j=1}^{m}r_{ij}L_nr_{ij} \quad \textbf{(7)}$$

When each value of r_{ij} is equal, entropy e_i reaches maximum and equals 1. Therefore the value of e_i satisfies $0\le e_i\le 1$. If the value of the entropy reaches maximum, the assessment factor contributes least to the system risk assessment. The weight of the risk factor can be determined by $1-e_i$.

So we get the weight value Φ_i

$$\Phi_i=\frac{1}{n-E}(1-e_i) \quad \textbf{(8)}$$

where

$E=\sum_{i=1}^{n}e_i$, and Φ_i satisfies: $0\le\Phi_i\le 1,\sum_{i=1}^{n}\Phi_i=1$.

4. THE CASE

According to the assessment model and items defined in Fig.1, assessment of security engineering ability of the whole system is divided into 3 levels.

Based on the items in different process areas of SSE-CMM we assessed an information system in e-Government system. From the analysis and calculation of information from the assessment, a corresponding subjection degree matrix is

obtained (Table.2).
At first the entropy coefficient of each assessment factors on the third level is calculated by equation (7): $M = (0.526, 0.714, 0.714, 0.714)$.

Table 2. Assessment matrix of single factors.

Assessment factors	CL0	CL1	CL2	CL3	CL4	CL5
PA02	0	0.1	0.4	0.5	0	0
PA03	0	0	0.2	0.4	0.3	0.1
PA04	0.2	0.3	0.4	0.1	0	0
PA05	0	0.2	0.4	0.3	0.1	0
PA01	0	0.3	0.4	0.3	0	0
PA07	0	0.2	0.2	0.3	0.2	0.1
PA08	0	0	0.2	0.2	0.4	0.2
PA09	0.3	0.4	0.3	0	0	0
PA10	0	0.1	0.3	0.3	0.2	0.1
PA06	0	0	0.2	0.3	0.3	0.2
PA11	0	0.1	0.3	0.3	0.2	0.1
PA12	0	0.4	0.6	0	0	0
PA13	0.3	0.5	0.2	0	0	0
PA14	0.1	0.3	0.5	0.1	0	0
PA15	0	0	0.1	0.2	0.5	0.2
PA16	0	0.1	0.4	0.5	0	0
PA17	0	0.3	0.4	0.3	0	0
PA18	0.1	0.5	0.4	0	0	0
PA19	0.6	0.3	0.1	0	0	0
PA20	0	0	0.5	0.4	0.1	0
PA21	0.3	0.5	0.2	0	0	0
PA22	0	0	0.4	0.6	0	0

Then the weight vector can be gotten by (8) as $A_{11} = (0.355, 0.215, 0.215)$.

The assessment factors set can be calculated by A_{11} and the subjective degree matrix in table.1.
The judge matrix of U_{11}= {PA02, PA03, PA04, PA05}:

$$B_{11} = A_{11} \cdot R_{11} = (0.355, 0.215, 0.215, 0.215) \cdot \begin{pmatrix} 0 & 0.1 & 0.4 & 0.5 & 0 & 0 \\ 0 & 0 & 0.2 & 0.4 & 0.3 & 0.1 \\ 0.2 & 0.3 & 0.4 & 0.1 & 0 & 0 \\ 0 & 0.2 & 0.4 & 0.3 & 0.1 & 0 \end{pmatrix}$$

In the same way we can get the synthetical judge matrix, (B_{11}, B_{12}, B_{13}).

After the uniform of (B_{11}, B_{12}, B_{13}), the judge matrix on the second level can be obtained, and in the same way we process above, the entropy coefficient method can be used to confirm the weight vector of U_1={U_{11},U_{12},U_{13}} and the judge matrix : B_1 = (0.0336，0.1182, 0.3016, 0.3039, 0.1604, 0.0825)
After uniformed it would be B_1' = (0.034， 0.118， 0.302，0.304, 0.160, 0.082). We deal with U_2, U_3 in the same way. Finally the final synthetical judge matrix we got B = (0.092, 0.213, 0.339, 0.227, 0.089, 0.040).

5. RESULT ANALYSES

The final result is (0.092, 0.213, 0.339, 0.227, 0.089, 0.040) which means the percentage of CL0, CL1, CL2, CL3, CL4, CL5. The project maturity of this system can be described as follow: CL0-CL5 each has proportioned 9.2%, 21.3%, 33.9%, 22.7%, and 8.9%; the maturity of the system can be seen in Fig.2.

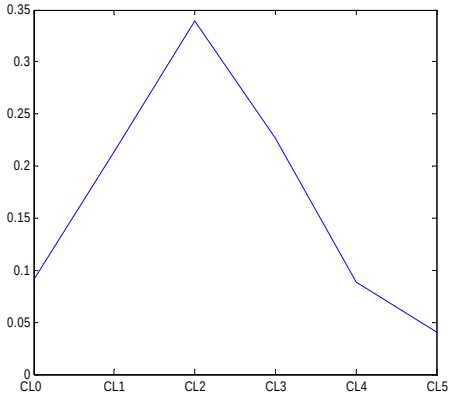


Fig.2. Assessment result of system project maturity of the case.

Based on the max subjective degree principle, the engineering ability of this system can be defined as CL2, planed and tracked, which means “understand what’s happening on the project before defining organization-wide processes” [8].

6. CONCLUSIONS

This paper proposes a security assessing method for e-Government system based on SSE-CMM and fuzzy comprehensive judgment. For calculating the weight of assessment factors, entropy-weight coefficient method is introduced. While applying this method into the assessment of the security ability of an e-Government system, the results tally with the actual situation.

REFERENCES

[1] Art, C., Gregory, B.W., “e-Government and Cyber Security: The Role of Cyber Security”, *Proceedings of the 39th Hawaii International Conference on System Science*, Hawaii (2006).
[2] Matia, W., Binaca V.B., “E-Government: Aspects of Security on Different Layers”, *Proceedings of the 12th International Workshop on Database and Expert Systems Application (DEXA’01)*, (2001).
[3] Cai, Y., Zhang, Y., “Risk Assessment of e-Government System”, *Computer Engineering and Application*, Computer Engineering and Application Press, Beijing, 2004, pp.155-160.
[4] Chen, J., Dai, Y., “Model of Information System Security Engineering Based on SSE-CMM”, *Computer Engineering, Editorial Board of Computer Engineering*, Shanghai, 2003, pp.35-36.
[5] Nie, X., Zhang, Y., D. Cai, “A Risk Assessment Method Based on AHP and Fuzzy Theory”, *Journal of Beijing Electronic Science and Technology Institute*, Beijing, 2005, pp.44-49.
[6] Liu, W., Liu, L., “Security Evaluation of E-Government Information System Based on SSE-CMM”, *Computer Engineering and Application*, Computer Engineering and Application Press, China, 2006, pp.223-226.
[7] Carnegie Mellon University, “SSE-CMM Project System Engineering Capability Maturity Model l® SSE-CMM® Model Description Document Version 3.0”, USA, 2003, pp.53-67.

Xiaorong Cheng was born in Handan city of Hebei province in China, 1963. She graduated from Hebei University. She is a professor and Doctor of Science. She has worked in North China Electric Power University since August 1985. She obtained the master's degree and doctor's degree from North China Electric Power University in 1994 and 2006. Her special fields of interest include computer network, information management and power line communication and she has been in charge of the development of several projects, such as the National Natural Science Foundation of China named Research of Broadband Power Line Communication Technology, Broadband Network Management Technology as well as Research of Network Security and so on.

Mei Li was born in Changxing city of Zhejiang province in China, 1981. She graduated from North China Electric Power University. Now she is studying at North China Electric Power University for master's degree. Her special fields of interest include information security and security assessment.

Wireless Networks VS Wired Networks in Security*

Xuanzheng Wang, Layuan Li, Chengzheng Wang
Department of Computer Science and Technology, Wuhan University of Technology
Wuhan, Hubei 430063.P.R.China
Email: wangxuanzheng138@163.com

ABSTRACT

This paper mainly introduces advantages and disadvantages of wireless and wire network from theory and practice. Besides, given us much advice about networks' security, we can take use of new technology of encryption isolation and firewall to make our networks running with high performance. Making sure our data avoid breaking and changing deliberately by hacker who invested by means of investing.

Keywords: Wireless Network, Wire Network, MAC, Rogue Access Points, VPN, WEP , WAP, Encryption, Isolation. Firewall

1. HAVE WIRELESS NETWORKS SURPASSED THE SECURITY OF WIRED NETWORKS

Wireless networks have long been known for being insecure. However, there has been so much emphasis on wireless network security, that in some ways, wireless network security is now better than the security used for wired networks. In this article, I will explain why this is the case and how to apply some of the wireless security techniques to your wired network.

It often seems to me that the term wireless network has become almost synonymous with the term insecure. Ever since wireless networks first started becoming popular, the Internet has been flooded with stories of wireless security nightmares. Rogue access points, parking lot spies, and Pringles can antennas have all been headaches that administrators of wireless networks have had to deal with. To make a statement that wireless networks are more secure than wired networks seems absolutely ludicrous, but is it true?

Let me start off by saying that I don't believe that wireless networks are more secure than wired networks as a whole. However, there are certain aspects of wireless network security that are superior to what's traditionally used on wired networks. There are two main reasons for this.

The first reason why some wireless security mechanisms are better than those used on wired networks has to do with the image problem that has plagued* wireless networks since the beginning. Wireless networks have always had a reputation for being insecure. Even so, there has been an unprecedented demand for wireless hardware. Being that wireless networks have become so popular, dozens of companies have invested big bucks into developing products and architectures designed to make wireless networks secure. Of course there are plenty of security products for wired networks as well, but the security solutions for wireless networks seem to me a little more unique and imaginative.

The other reason why wireless networks tend to be more secure than wired networks in some regards is because of the overall philosophy behind the network. For example, imagine that you created a small network with a Windows 2003 Server and five workstations running Windows XP. The machines are all brand new and no one has touched any of the hardware except for you. You have installed all of the operating systems, applications, and security patches. The PCs have never been exposed to end users or to the Internet. The question that I am asking you is do you trust the workstations on your network? Of course you do.

Now, let's turn the situation around a little bit. Let's assume that everything is the same as before, but the server and the PCs are all a part of a wireless network rather than being wired to a switch. Assuming that your wireless access point is running an out of the box configuration, do you trust the PCs on your network? Hopefully, you said no because with a generic wireless network configuration, you have no way of guaranteeing that the PCs connecting to your wireless network are really your PCs. Sure, your PCs are connected to the wireless network, but your neighbors can also connect to your network as well.

The point that I am trying to make is that the overall philosophy behind wired networks vs. wireless networks is trust. On a wired network, the hardware is under the direct control of the network administrator, and therefore, the overall attitude toward the workstations tends to be one of trust. On a wireless network, it is a well known fact that someone could sit in the parking lot with a laptop and access your wireless network. Therefore, the general attitude toward wireless workstations tends to be one of extreme distrust.

This difference in attitude often causes the same administrators who go to extreme lengths at securing a wireless network, to almost neglect wired network security. Let me ask you another question though. Are there any unused network jacks or unused switch ports in your office? If someone was able to sneak into the office and plug a laptop into one of these unused jacks, would you still have the same level of trust in the hardware on your wired network? A wireless local area network (WLAN) is the linking of two or more computers with Network Interface Cards (NIC) through a technology based on radio waves. All devices that can connect to a wireless network are known as stations. Stations can be access points (AP), or clients. Access points are base stations for the wireless network. They receive and transmit information for the clients to communicate with. The set of all stations that communicate with each other is referred to as the Basic Service Set (BSS). Every BSS has an Identification known as a BSSID, also known as the MAC address, which is a unique identifier that is associated with. every NIC. For any client to join a WLAN, it should know the SSID of the WLAN, therefore, the access points typically broadcast their SSID to let the clients know that an AP is in range. Data streams, known as packets, are sent between the Access Point, and it's clients. You need no physical access to the network or its wires to pick up these packets, just the right tools. It is with the transmission of these packets that pose the largest security threat to any wireless network. One of the most basic features included in most wireless access points is a list of workstations that are allowed to access the wireless network.

* This work is supported by the National Natural Science Foundation of China (No. 60672137) and Specialized Research Fund for the Doctoral Program of Higher Education of Higher Education of China (No. 20060497015)

This feature allows you to enter the MAC address of each wireless NIC that your company owns. However, sometimes this feature may be used by hacker who constantly spied user's information, especially NIC's MAC address. Once hacker gains this important information, He will take use of user's identity to do anything he wants including snooping and violating important information. The Figure 1 is the hacker rogues access point process by using user's private information. By the way, if someone attempts to connect to your network, the access point checks to see if the NIC's MAC address is allowed. If not, then the connection is denied.

This technology isn't absolutely perfect though. There are still a couple of ways that a hacker could breach the wireless network. For example, some NICs allow you to set the MAC address to an address of your choice. A hacker could spy on the network, get the address of a valid NIC and then assign that

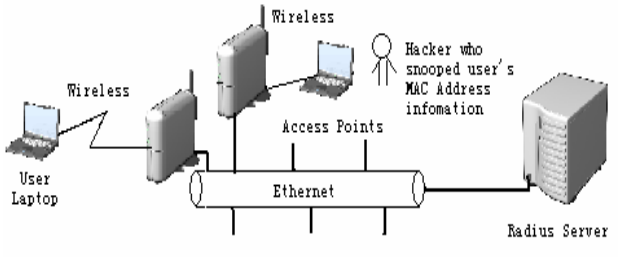


Fig.1. Hacker rogue access points process

address to their own NIC. It is also possible that a hacker could steal one of your NICs and use it to gain access to the network

At the same time though, you have to remember that a media access control filter is not your only line of defense. It is an excellent starting point though. The problem is that most wired networks do not have such a feature in place. Administrators assume that every PC on the wired network has a right to be there, so there's no reason to implement a media access control filter.OK, I'll admit that the chances of someone just walking in off the street and plugging a laptop into an empty network jack are pretty slim. Think about this though. Rogue access points have been a huge problem for corporations. There have been countless situations in which a company doesn't want a wireless network, but an employee does, so they set up their own access point. There have also been cases in which an employee is mad because they weren't granted access to the wireless access point, so they set up their own.

An employee doesn't need a spare network jack to set up a rogue access point. Access points usually have a mini-hub built in. A user could just unplug their PC and plug the access point into the network jack that the PC had been using. They can then plug their PC into the access point. So what does this have to do with media access controls? Most wireless access points have a MAC address of their own. Therefore, if your wired network had a MAC address filter in place, then the rogue access point would never be able to gain access to the rest of the network.

2. ENCRYPTION

Would you communicate across a wireless network without using encryption? Of course not, but many of the wired networks allow the majority of communications to go unencrypted. Wired networks are just as prone to eavesdropping as wireless networks are. The only difference is that wireless networks can be snooped on by outsiders, and snooping on a wired network requires a physical connection. Even so, I have seen plenty of instances in which an employee uses a protocol analyzer to spy on co-workers. So, we should make use of encryption algorithm to encrypt message. Only in this way, the possibility of message which is snooped is very small. About encryption algorithms are too many, such as DES, RC4, MD5, RSA. The figure.2 introduces date encryption process.

Microsoft began offering IPSec encryption with Windows 2000, and continues to offer it in Windows Server 2003 and in Windows XP. IPSec is that one kind opens the standard frame, can swear to communicate by letter by the fact that the IP network realizes the safe private interests secret. IPSec VPN uses the service that the IPSec inner defines, to ensure that Internet waits for common the privacy protection having caught with a net data communication, completeness and attestation. IPSec owns pragmatic application. They place IPSec at pure version 802.11 wireless rate of floabove, to protect WLAN. When deploying IPSec in WLAN environment, IPSec places at the each platform PC linking with wireless network, the consumer needs the wired net to build IPSec passage then , arrives at rate of flow to be transmitted. The filter is used to prevent wireless rate of flow from getting to the destination outside the VPN gateway and the DHCP/DNS server. IPSec is used to realize IP rate of flow privacy protection, attestation and to guard against the rebroadcast function. Keep secret nature comes true by the encryption, encrypt the variation (be called three DES (3 DES)) using the data encryption standard (DES) , is to use three secrets key to carry out the triple encryption on the data. Although IPSec is used to realize the data privacy protection mainly, standard expansion also can be used for consumer attestation and be authorized, and as IPSec process part, however, many companies choose to only encrypt traffic flowing between servers. Although there are certainly exceptions, the bulk of the traffic flowing between servers and workstations is typically not encrypted. Concerning wireless networks' encryption of message, there are many

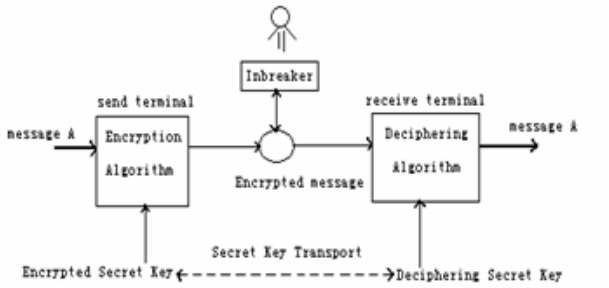


Fig.2. Date Encryption Model

different encryption technology which contain WEP (Wireless Equivalent Privacy),802.1X protocol, VPN(Virtual Privacy Network),SSID,AP. Today most of enterprises use WEP to encrypt message which transmits on internet, WEP is very popular in our modern society. Let's understand the WEP encryption process simply, WEP was designed to protect a wireless network from eavesdropping, but it soon became apparent that due to myriad flaws, WEP's privacy was not at all equivalent to that of a wired network. Therefore, it wasn't long before a new technology called WPA — Wi-Fi Protected Access — debuted to address many of WEP's shortcomings. WPA has been a mainstream technology for years now, but WEP remains a standard feature on virtually every wireless router on store shelves today. Although it's mainly there for backward compatibility with the oldest hardware, if reports and

studies are accurate, a significant percentage of WLAN operating today are still using outdated and insecure WEP for their encryption. From the Fig 3. We can know WEP frame encryption process.

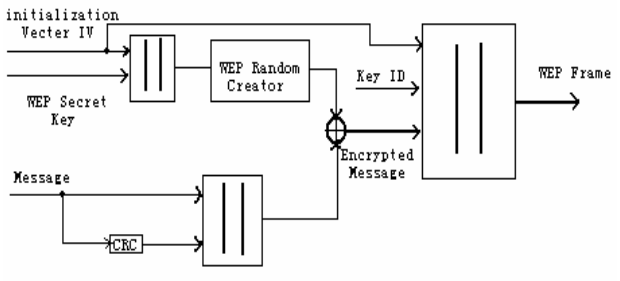


Fig.3. WEP frame encryption process

Every encrypted packet contains a 24 or 48 bit IV, depending on the type of encryption used. Since the pre-shared key is static and could be easily obtained, the purpose of the IV is to encrypt each packet with a different keys, the problem with this method is that the Initialization Vectors are not always the same. In theory, if every IV was different, it would be nearly impossible to obtain the network key; this is not the case. WEP comes with a 24 bit IV; therefore, giving the encryption 16 million unique values that can be used. This may sound like a large number, but when it comes to busy network traffic, it's not. Every IV is not different; and this is where the issues arise. Network hackers know that all the keys used to encrypt packets are related by a known IV; therefore, the only change in the key is 24 bits. Since the IV is randomly chosen, there is a 50% probability that the same IV will repeat after just 5,000 packets; this is known as a collision. WEP - Wired Equivalent Privacy - comes in 3 different key lengths: 64, 128, and 256 bits, known as WEP 64, WEP 128, and WEP 256 respectively. WEP provides a casual level of security but is more compatible with older devices; therefore, it is still used quite extensively. Each WEP key contains a 24 bit Initialization Vector (IV), and a user-defined or automatically generated key; for instance, WEP 128 is a combination of the 24 bit IV and a user entered 26 digit hex key. WPA – WiFi Protected Access - comes in WPA, and was created to resolve several issues found in WEP. Both provide you with good security; however, they are not compatible with older devices and therefore not used as widely. WPA was designed to distribute different keys to each client; however, it is still widely used in a pre-shared key mode, in which every client has the same pass phrase. To fully utilize WPA, a user would need an 802.1x authentication server, which small businesses and typical home users simply cannot afford. WPA utilizes a 48 bit Initialization Vector (IV), twice the size of WEP, which combined with other WEP fixes, allows substantially greater security over WEP.

A couple of years ago, conventional wisdom stated that most workstation traffic should not be encrypted because of the burden that encryption places on the network. The encryption and decryption process consumes processing power, and encrypted packets typically consume more network bandwidth. But today human's attitudes changed.

Although these may have been valid arguments at one time, I believe that the time has come to encrypt all network traffic. Network cards exist that can handle the encryption and decryption process without having to burden the processor. Likewise, gigabit network cards have become cheap enough that the extra bandwidth required by encrypted packets should no longer be a huge issue.

3. ISOLATION

One of the other ways that wireless network security has surpassed wired security is in the way that it is isolated. In many companies, anything coming in through a wireless access point is automatically assumed to be non trustworthy, until the sender can prove otherwise. Because the air waves are assumed to be an insecure medium, wireless traffic is handled in a different way than wired traffic. Companies will typically establish a VPN for wireless users.

The idea is that when a user attaches to a wireless network, they are completely isolated from the rest of the network until they have been authenticated. Often, the authentication mechanism isn't even allowed direct access to a domain controller. Instead, a RADIUS server is typically used to authenticate wireless users. Once authentication has been established, then the user communicates with the network through a secure tunnel.

What is interesting about this is that the VPN like connection uses its own encryption. The VPN is considered as the most security among all the wireless networks transmittal. The figure.4.describes the IP-VPN's application about wireless networks' message transmittal in modern society. We start to encrypt the message, then, message authentication and IP encapsulation used IP-VPN equipments, the last the message disposed right now transmits in special tunnel instead of public IP network. The special tunnel is secure, virtual and exclusive. So the message transmits in that is absolutely safe. It is very difficult to snooped by hacker. The remainder is as the same. Message's security will cost some time and money. the wireless signal is already encrypted by using WPA or something similar. This means that legitimate wireless traffic is double encrypted, using two completely different encryption protocols.

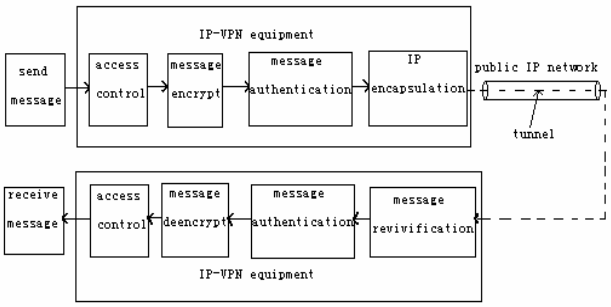


Fig.4. VPN model

In my opinion, isolating segments of a wired network and requiring RADIUS authentication is probably overkill in most cases. It is a good example though of a way in which wireless security mechanisms are more stringent than those used on wired networks.

4. FIREWAll

In the wireless networks, the firewall built into your router prevents hackers on the Internet from getting access to your PC. But it does nothing to stop people in range of your Wi-Fi signal from getting onto your network--and with the latest high-performance equipment, your Wi-Fi signal could reach clear down the block. Without encryption and other protective measures, anyone can use readily available tools to see all your Wi-Fi traffic. Disregarding being to own wireless network

LAN enterprise , still not owning, the city is threatened by the safety that Wi-Fi brings about, but at present the firewall and VPN fail-safe system have no way to protect them. Besides LAN places your wireless in the enterprise fire prevention wall go neither. Installation and cost are easily cheap. Wi-Fi cut-over may lead into and deploy by yourself employee, Be to there be no evil intention's generally, these switch in point that the visit not authorizing is called burning, becoming a hacker intrudes into your network entrance , uses your important assets such as your business , customer , product and the secret information serving suffer attack easily. Other threatens point of attack, accepts including refusing to serve AP that (DoS) attack and your self mistake deploy may become extra YI. he firewall protecting tradition by the fact that your fire prevention wall an VPN accomplish a network monitors wired rate of flow only , does not have the observation force to wireless rate of flow. Leave entrance to hacker in the network that all safety intervenes in without authoritative switch in by outflanking to you. Even if your business is not wireless LAN, your upper wireless laptop customer holds the network linking adjoining also possibly, Self and the network is opened to the outside world giving malicious attack person. Enterprise level SG Enterprise is entire wireless of one kind invade check and protect a scheme, include a server and wireless sensory equipment, what be come into being wireless being able to be no discontinuous monitoring the wireless channel , using personal influence with Wi-Fi preventing possessions from not having authorized invades. SG Enterprise SG Enterprise is that a enterprise level wireless covers the fire prevention wall as with a net resolving a scheme , comes to resolve these problems by providing entire Wi-Fi fire prevention wall , provides the enterprise channel protecting, and attaching importance to in you with identical all-round of wired fire prevention wall.

5. CONCLUSIONS

Although I don't believe that wireless networks are more secure than wired networks as a general rule, there's little question that a greater emphasis is placed on wireless security than on wired security. If you are really concerned about the security of your wired network, then it may be worth taking a look at the security mechanisms used on your wireless network and seeing if any of those techniques can be adapted to your wired network. I am sure that with the science and technology's development our human deal with these problems about wireless and wire networks in security well.

REFERENCES

[1] Lao Jinling, *Network security and management*. [M] Beijing: Higher education publishing house 2003

[2] .LI Layuan, "Computer network technology": [M] Defense industry publishing house 2004

[3] Lei Zhen, *Network engineer course*. [M] Beijing: Qinghua University publishing house 2004

[4] Qi Ming, *Network security and security*. [M] Beijing: Higher education publishing house 2004

[5] Guo Jun, *Network management*. [M] Beijing: Beijing posts and telecommunications university publishing house 2005 *Saidi.net Computer user* [J] 2002.04.18

[6] Bai Yien, *Computer network foundation and application. [M] Heilongjiang*: Hall guest industrial university publishing house 2003

Xuanzheng Wang is a graduate student in School of Computer Science & Technology, Wuhan University of Technology. He got his bachelor's degree in Anyang Normal College of in 2006. My main research interests are in computer networks, network and information security.

Layuan Li, was born in Hubei, China on 26 February 1946.He received the BE degree in Communication Engineering from Harbin Institute of Military Engineering, China in1970 and the ME degree in Communication and Electrical System from Huazhong University of Science and Technology ,China in 1982. He academically visited Massachusetts Institute of Technology (MIT),USA in 1985 and 1999, respectively. Since 1982,he has been with the Wuhan University of Technology (WUT), China, where he is currently a professor and Ph.D tutor of Computer Science, and editor in chief of the Journal of WUT. He is Director of International Society of High-Technol and paper reviewer of several IEEE Transactions and Jounals. He was the head of the Technical Group of Shaanxi Lonan PO Box 72,Ministry of Electrical Industry, China from 1970 to 1978. His research interests include computer networks, protocol engineering and image processing. Professor Li has published over one hundred and fifty technical papers and is the author of six books. He also was awarded the National Special Prize by the Chinese Government in 1993.

Chengzheng Wang is a senior school teacher. He is teaching chemistry in Jiaozuo city Henan province, he got his bachelor's degree in Anyang Normal College of in 1991. He main research interests are in chemistry and network and information security.

Image Double Encryption Method Based on Chaotic Map and DWT *

Shuguo Yang[1,2], Shenghe Sun[2], Chunxia Li[1]
[1]Qingdao University of Science & Technology Qingdao, ShanDong, 266061, China
[2]Harbin Institute of Technology, Harbin, HeiLongJiang, 150001, China
Email: ysg_2005@163.com

ABSTRACT

Image encryption becomes more and more important with the development of the network technology and the multimedia technology. A novel and secure image encryption method based on Chaos map and DWT is described at length in the paper. Firstly, we introduce two coupling chaotic maps to scramble an original image, and receive the scrambled image. Secondly, we transform the scrambled image by DWT. At the same time, we introduce a chaotic map again, and then we encrypt the wavelet coefficients of the scrambled image in DWT domain. In the whole process we use three chaotic maps, five keys and encrypt the image twice. Finally, we do many experiments and the experimental results prove our method to be secure.

Keywords: Image Scrambling, Image Encryption, Chaotic Map, Secret Key, DWT

1. INTRODUCTION

With the development of the network technology and the multimedia technology, the process of image transmission becomes more and more simple. On the one hand people can transmit and receive the images easily; on the other hand infringers also get images easily. So the issue of image information security becomes more and more urgent, important and necessary.

Recently, the researchers pay much attention to chaos encryption system. Because the chaotic system is sensitive to the initial value and control parameter, and the chaotic sequences have many fine characteristics such as random-like, noise-like, broad spread spectrum, and be reproduced easily, it is used to the image information encryption frequently. The image chaotic encryption method is becoming a novel kind of encryption method, also a hot spot of research.

Up to now, people proposed many image encryption methods, which can be divided into two categories: one is the spatial domain method and another is the frequency domain method. The advantages of the spatial domain method are that it is handled easily and couldn't bring extra image distortion etc, but its disadvantages are that its computation is complicated and its encryption effect is not fine. For example, Jui-Cheng Yen and Jiun-In Guo proposed some schemes such as BRIE[1]、CKBA[2], HCIE[3], TDCEA[4], RSES[5], which use Logistic map($x_{k+1} = \mu x_k (1 - x_k)$, $3.5699456\cdots < \mu \le 4$) to produce chaotic PRNG, and then use PRNG to disorder the point and the gray-scale value of image pixels. These methods are easy to work and don't bring much distortion to image. Because they don't resist to known/chosen plaintext attack, they aren't secure [6]. The frequency domain methods are robust and can counteract interference, so their encryption results are better than those of the spatial domain methods. For example, Kai-Xiang Yi and Xin Sun proposed a good method for image scrambling using chaotic sequences in DCT domain [7]. Hua-Ning Shan and Zhi-Quan Wang proposed an image scrambling method that relies on chaotic cat map in DWT domain and has a good encryption result [8]. Xian-Dong Yin and Jun Yao reported an image encryption method that encrypts the discrete wavelet coefficient matrix of the image using the chaotic sequences and has simple keys [9]. After analyzing many image encryption methods in frequency domain, we find the image encryption methods in DWT domain are better than those methods in DCT domain. So the image encryption methods in DWT domain are promising and have a happy future.

The paper reports an image double-encryption method based on the chaos theory and the discrete wavelet transform. Firstly, we scramble the image by two coupling Logistic maps. Secondly, we transform the scrambled image by discrete wavelet transform and encrypt the coefficients of the transformed image again. Finally, we do many tests and the experimental results prove our method to be secure, robust and effective.

2. DOUBLE COUPLING LOGISTIC MAPS

Chaos is a kind of complex dynamic behavior of non-linear systems. The Logistic chaotic map is a discrete iteration system which can be formulated as:

$$x_{n+1} = \mu x_n (1 - x_n), n = 0,1,2,\cdots$$

Where x_0 is the initial value of the iteration system, x_n is the value of the chaotic sequence, parameter μ can control the behavior of non-linear system, and $0 \le x_n \le 1$, $0 < \mu \le 4$. The map can be chaotic when $3.5699456\cdots \le \mu \le 4$.

In order to enhance the random and encryption characters of the chaotic sequence, we adopt two Logistic maps and mix them by controlling parameters each other. The coupling Logistic maps are as follows:

$$\begin{cases} x_{n+1} = \mu_x x_n (1 - x_n) \\ y_{n+1} = \mu_y y_n (1 - y_n) \end{cases} \quad (1)$$

Where μ_x and μ_y are parameters, x_n and y_n are the values of the chaotic sequence. The value of parameter μ_x is 3.9 or 3.9888 and the value of parameter μ_y is 3.944444 or 4.0[10]. The parameters are altered according to the following formulas:

$$\mu_x = \begin{cases} 3.9 & 0 < y_j \le 0.5 \\ 3.9888 & 0.5 < y_j \end{cases}$$
$$\mu_y = \begin{cases} 3.9444 & 0 < x_i \le 0.5 \\ 4.0 & 0.5 < x_i \end{cases} \quad (2)$$

According to Eq. (1) and Eq. (2), we can produce the chaotic sequences $\{x_1, x_2, \cdots, x_m\}$ and $\{y_1, y_2, \cdots, y_n\}$.

* This project is funded by the research fund for doctor of Qingdao University of Science & Technology and Hei Long Jiang Province Natural Science Fund (TF2005-09).

3. THE IMAGE SCRAMBLING METHOD BASED ON CHAOTIC MAPS

The image scrambling is a common method for image information encryption. It disorders the image information, so the unauthorized people can't receive any true information, but the legal owner could recover the original image from the scrambled image. Many methods for image scrambling are proposed up to now. For example, Xin Sun et al. researched a kind method of image scrambling based on chaotic system [7]. Sen Bai et al. proposed a kind of image information hiding method based on knight stroll transform [11]. Wei Ding et al. proposed a kind of image scrambling method based on Arnold transform [12]. Dong-Xu Qi and Dao-Shun Wang et al. discussed Arnold and Fibonacci-Q transforms, and proposed a novel kind of non-linear transform to disturb image information [13, 14]. But their method is complicated. Sen Bai and Gui-Bin Zhu et al. reported a kind of image scrambling method based on affine transform [15, 16].

We suppose an original image is I whose size is $M \times N$ (in pixel), and then the image could be denoted as:

$$\mathrm{I} = F(i, j)\ (0 \le i \le M; 0 \le j \le N) \qquad (3)$$

Where (i, j) denotes the position of a pixel point, $F(i, j)$ denotes the image data of the pixel point (i, j).

The process of scrambling the original image is:

(1) Setting initial values of the chaotic systems in Eq. (1) to be x_0 and y_0, we can produce two chaotic sequences $x_1, x_2, \cdots, x_M$ and $y_1, y_2, \cdots, y_N$. Then we range two chaotic sequences by magnitude and get the sequences $x'_1, x'_2, \cdots, x'_M$ and $y'_1, y'_2, \cdots, y'_N$. Each x_i $(i = 1,2,\cdots, M)$ is corresponding to a integer $w_{x_i} (\in \{1,2,\cdots, M\})$ which is the order of x_i in the sequence $x'_1, x'_2, \cdots, x'_M$, at the same time, each y_j $(j = 1,2,\cdots, N)$ is corresponding to a integer $w_{y_j} (\in \{1,2,\cdots, N\})$, so each (x_i, y_j) is corresponding to (w_{x_i}, w_{y_j}).

(2) Disordering the original image data.

Because each pixel point (i, j) of the original image is corresponding to (x_i, y_j), and each (x_i, y_j) is corresponding to (w_{x_i}, w_{y_j}), so each (i, j) is corresponding to (w_{x_i}, w_{y_j}). We replace the image data $F(i, j)$ by the image data $F(w_{x_i}, w_{y_j})$, and then we get the scrambled image I′.

In above-mentioned process, the initial values of the chaotic maps can be protected as the secret keys $(K_1 = x_0, K_2 = y_0)$.

4. THE IMAGE CHAOTIC ENCRYPTION MEHTOD IN DWT DOMAIN

The DWT is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency and represent an octave-band decomposition. By DWT, we have three parts of multiresolution representation (MRR) and a part of multiresolution approximation (MRA)[17]. The subbands labeled LH_1, HL_1, and HH_1 of the MRR represent the finest scale wavelet coefficients. To obtain the next coarser scale of wavelet coefficients, the subband LL_1 (that is, MRA) is further decomposed and critically subsampled.

Giving an original image I whose size is $M \times N$, we can get a scrambled image I′ whose size is also $M \times N$ based on the above method, and then we encrypt image I′ as follows:

(1) If $M \times N$ isn't an integer multiple of 8×8, we extend the boundaries of the image I′ (the value of the added pixel point is 0) and then we decompose the image I′ by DWT. As an example, Fig. 1 shows the image I′ decomposed into ten subbands for three scales:

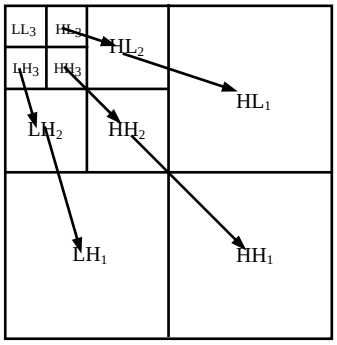


Fig.1. Octave decomposition of an image

(2) We can divide the wavelet coefficients into four groups: low frequency zone LL_3, horizontal zone(HL_3, HL_2,HL_1), vertical zone(LH_3, LH_2, LH_1) and diagonal zone(HH_3, HH_2,HH_1) (Fig.1), and then arrange these wavelet coefficients to an one-dimension array $d(k)$ $(k = 1,2,\cdots, n)$ based on wavelet zero tree scanning method(Fig.2) as follows:

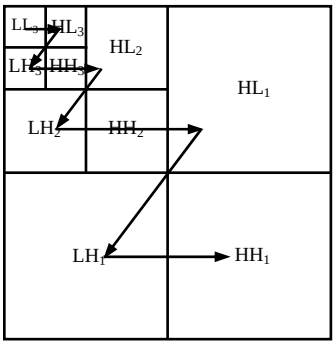


Fig.2. The order of scanning the wavelet coefficients

(3) We produce chaotic sequence $x(k)(k = 1,2,\cdots, n)$ by the following formula:

$$x(k+1) = 1 - \mu x^2(k) \qquad (4)$$

Where $x(0)$ is a preset initial value, $x(k) \in (-1,1)$ $(k = 1,2,\cdots, n)$, μ is a parameter. The maps can be chaotic if the parameter μ is selected properly.

(4) In order to make the wavelet coefficients change adaptively, we adopt the following formula to modify every wavelet coefficient of image:

$$d'(k) = d(k)(1 + x'(k)) \qquad (5)$$

Where $x'(k)$ is derived from $x(k)$ when we set the number of significant figures of $x(k)$ be λ, $d(k)$ is the original wavelet coefficient, $d'(k)$ is the new wavelet coefficient ($k = 1,2\cdots, n$).

(5) We transform the image I′ by IDWT based on coefficient

$d'(k)$ ($k = 1,2\cdots, n$), then we receive the encrypted image II′.

In above-mentioned process, we introduce three keys ($K_3 = \mu, K_4 = x(0), K_5 = \lambda$), then we get five keys $(K_1, K_2, \cdots, K_5)$. Because the ranges of these keys are very wide, the works searching them are very difficult. At the same time, the changes of the wavelet coefficients can bring influence on the whole image, so the effect of image encryption is well.

The block diagram of the image encryption process is as follows:

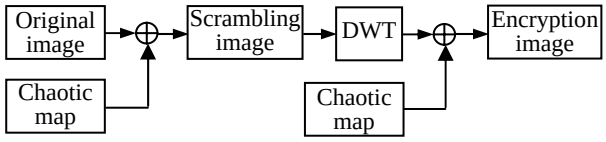


Fig.3. Scrambling image

5. EXPERIMENTAL RESULTS

To test our encryption technique for robustness and security, we conducted many experiments on a standard test image Lena.bmp (Fig.4), whose size is 256×256. We set x_0 to be 0.01 and y_0 to be 0.101 in Eq. (1), then we received the chaotic pair $(x_i, y_j)(i, j = 1,2,\cdots,256)$. We rearranged $F(i, j)$ according to the method in step2 of section 3, and then we obtained the scrambled image I′ (Fig.5). After decomposing the image I′ in 3 levels using wavelet basis, we rearranged the wavelet coefficients and got a one-dimension array $d(k)(k = 1,2,\cdots,65536)$. We set μ to be 1.58 and set $x(0)$ to be 0.1 in Eq. (4), received the chaotic sequence $x(k)$, $(k = 1,2,\cdots,65536)$ and then calculated $d'(k)(k = 1,2,\cdots, 65536)(\lambda = 3)$. We transformed the image I′ by IDWT according to coefficient $d'(k)$, and then we obtained the encrypted image II′ (Fig.6).

Fig.4 Original image I

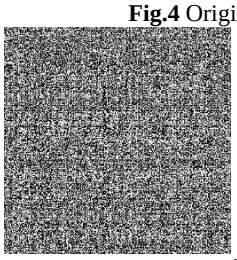


Fig.5 Scrambled image I′

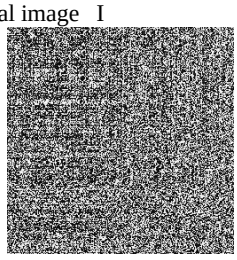


Fig.6 Encrypted image II′

Test 1. Image Decryption Test

Firstly, we decomposed the encrypted image II′ (Fig.6) in 3 levels using wavelet basis and received the coefficient sequence $d'(k)(k = 1,2,\cdots,65536)$. Secondly, we set μ to be 1.58 and set $x(0)$ to be 0.1, obtained the sequence $x(k)$ and $x'(k)$ based on the Eq.(4), and then received the coefficient $d(k)$ ($\lambda = 3$) according to the Eq. (5). Finally, we transformed the image II′ by IDWT according to the coefficient $d(k)$ and received the image I′. We processed the image I′ according to the inverse process of image scrambling, and then we got the decrypted image (Fig.7).

Fig.7 Decrypted image

Comparing the decrypted image (Fig.7) to the original image (Fig.4), we drew a conclusion that they are about the same if we adopt the right key when we decrypt the encrypted image, that is, the method is secure.

Test 2. Security Test

We conducted the encrypted image II′ (Fig.6) when μ is 1.580001 and $x(0)$ is 0.1 according to the process in test 1($\lambda = 3$), then we obtained decrypted image (Fig.8). According to the same process, we obtained another decryption image (Fig.9) when μ is 1.58 and $x(0)$ is 0.100001 ($\lambda = 3$).

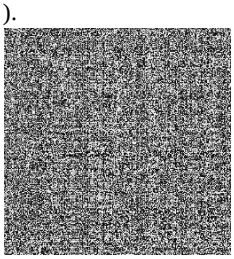


Fig.8. Decrypted image ($\mu = 1.580001, x(0) = 0.1$)

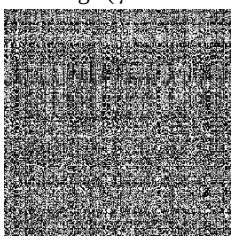


Fig.9. Decrypted image ($\mu = 1.58, x(0) = 0.100001$)

Comparing two decrypted images (Fig.8 and Fig.9) to the original image (Fig.4), we drew a conclusion that the decrypted images are very different from the original image if we used the error keys when we decrypted the encrypted image. That is, if we wanted to receive the right image information, we must find the right keys. Because the ranges of keys are very wide and the work of searching for keys is hard, the method is secure.

Test 3. Compression Test

After setting threshold T_0 to be a proper value which ensures the compression effect, we carried out discrete wavelet compression to the encrypted image II′ (Fig.6) by abandoning those coefficients whose value is smaller than T_0 and reserving the left coefficients. We received the compression image and decrypted it, so we obtained the decrypted image (Fig.10).

Fig.10. Decrypted image after being compressed

Test 4. Adding Noise

We added Gauss noise whose variance is 4 to the encrypted image II′ (Fig.6), and decrypted it. The decrypted image is as follows:

Fig.11. Decrypted image after adding noise

6. CONCLUSIONS

The proposed method includes two key works: scrambling image and encrypting image, and uses three chaotic maps (two coupling chaotic maps and one chaotic map) and changes wavelet coefficients adaptively in DWT domain. It has five keys in the whole process which are found difficultly and the changes of the wavelet coefficients can bring influence on the whole image. So this image encryption method is secure, which is testified by many test results.

REFERENCES

[1] Jui-Cheng Yen, Jiun-In Guo, "A new image encryption algorithm and its VLSI architecture," in *Proc. IEEE Workshop on Signal Processing Systems*,1999,pp.430-437.

[2] Jui-Cheng Yen, Jiun-In Guo,"A new chaotic key-based design for image encryption and decryption," in *Proc. IEEE Int. Symposium on Circuits and Systems*, 2000, pp.49-52.

[3] Jui-Cheng Yen, Jiun-In Guo,"Efficient hierarchical chaotic image encryption algorithm and its vlsi realization,"in *lEE ProcVis. Image Signal Process*, 2000, 147(2), pp.167-175.

[4] Jui-Cheng Yen, Jiun-In Guo, "Design of a new signal security system," in *Proc. IEEE Int. Symposium on Circuits and Systems*, IEEE, 2002,(IV),pp.121-124.

[5] Hun-Chen Chen, Jui-Cheng Yen, Jiun-In Guo, *Design of a new cryptography system.Springer-Veriag*,2002, 2532, pp.1041-1047.

[6] Hai-Ying Nie, Chan-Yan Zhu,C*haotic Image Encryption Algorithm Resilient to Known/Chosen Plaintext Attrack .information security and communication encryption,* 2006, (10),pp.125-127.

[7] Xin Sun, Kai-Xiang Yi, You-Xian Sun, "Image Encryption Algorithm Based on Chaos System[J]," in *Jounal of Computer-aided Design & Computer Graphic*, 2002, 14(2), pp.136-139.

[8] Hua-Ning Shan, Quan-Zhi Wang, Guo-Qing Wang et al,"A Image Chaos Encryption Method Based On DWT [J],"in *Computer Applications*,2003,23(6), pp.199-200.

[9] Dong-Xian Yin, Jun Yao, Zai-Ming Li,"Image Encryption Algorithm Based on Transformation and Chaotic Sequences [J],"in *Computer Engineering and Applications*,2004,40(34),pp.12-14.

[10] De-Ling Zheng, Geng Zhao, Guo-Bao Xu,"Logistic Map Digital Stream Chaos Singularity Terminal and Parameters[J],"in *Journal of Beijing University of Science & Technology*,2002,24(3),pp.350-352.

[11] Sen Bai, et al,"Digital Image Detail Encryption Method Based on Knight Stroll Transform [J],"in *Journal of Image and Graphics*,2001,6(11), pp.1096-1100.

[12] Wei Ding,et al,"Digital Image Scrambling Method Based on Arnold Transform [J],"in *Journal of Computer- aided Design & Computer Graphic*,2001, 13(4),pp.338-341.

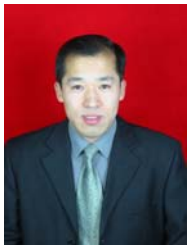
[13] Dong-Xu Qi, etal,"A Novel Scrambling Transform and Its Applications in Image Information Encryption [J],"in *China Science (E)*,2000,30(5),pp.440-447.

[14] Dao-Shun Wang, et al,"Two Kind of Digital Image Non-linear Transforms and Their Periods [J],"in *Journal of Computer-aided Design & Computer Graphic*, 2001, 13(9),pp.828-833.

[15] Sen Bai, et al,"The Character and Application of Sub-affine Transform [J],"in *Journal of Computer-aided Design & Computer Graphic*,2003, 15(2),pp.205-208.

[16] Gui-Bin Zhu,et al,"A Digital Image Scrambling Encryption Method Based on Affine Transform[J],"in *Journal of Computer-aided Design & Computer Graphic*,2003,15(6),pp.711-715.

[17] S.G. Mallat, "A theory for Multiresolution signal decomposition: The wavelet representation,"in *IEEE Trans. Pattern Anal.& Mach.* Intell., vol.11,no.7,pp. 674-693,1989.



Shuguo Yang is a doctor and Professor of Mathematic and physical college of Qingdao University of Science & Technology. He graduated from Harbin Engineering University; He has published over 40 Journal papers, edited five books. His research interests are in Digital image process, network security and multimedia technology.

Security Access Model of P2P File-Sharing System

Jinsong Wang[1,2] , Ning Wang[1] , Weiwei Liu[1], GongYi Wu[2]
[1]School of Computer Science and Technology, TianJin University of Technology, 300191, China
[2]Dept. of Computer Science, Nankai University, Tianjin 300071, China

ABSTRACT

Nowadays P2P file-sharing systems are short of effective security mechanism. In this paper, we design and implement a security access model of P2P file-sharing system. It uses trust mechanism to keep provider's resources credible and security. And we select SPKI (Simple Public Key Infrastructure) to authorize the peers and to control access flexibly, moreover, we add degree of trust and contribution value together to control re-delegating authorizations that made up SPKI's insufficiency .Besides these, we design incentive mechanism to the model that not only reduces free-riders, but also solves the asymmetry in the download and upload traffic.

Keywords: Peer-to-Peer, Trust Model, Incentive Mechanism, Distributed Authorization, Free-Rider

1. INTRODUCTION

P2P becomes the focus of attentions for many researchers in the recent years. At the same time, P2P network is yet frail. Because it's open and anonymous in P2P system, peers have no need to take responsibility for what they have done .So many security problems in P2P system need to be solved immediately.

The main problems are the following four issues:
1. Some hackers spread bad resources, i.e.: worms and viruses.
2. Free-rider, many peers download files from others, while they don't permit other peers to get access to their own files. As the consequence, the whole system's performance will degrade considerably, which makes everyone worse off .3. Traditional access control is no longer to fit P2P network. PKI can be used only to authenticate the clients of services, because they can't be used to properly authorize the peers and control access to services.

In order to improve above problems, we put forwards a security access model of P2P file-sharing system that combined PGP Trust Model, incentive Mechanism and SPKI together.

The rest of this paper is arranged as follows: Section Ⅱ: discusses the related work. Section Ⅲ: presents the security access model. Section Ⅳ: describes our method and implementation process. Section Ⅴ: draw a conclusion.

2. RELATED WORK

In order to solve the problem whether the files are credible and to avoid hacker from spreading bad resource, trust mechanism is put forwards. Two types of schemes based on trust mechanism were proposed recently: overall trust model and local trust model. The overall trust model also can be divided into two groups .One [1] [2] is that peers can get the feedbacks both good and bad, and then compute the degree of trust through simple algorithm. But this method can't deal with the unfair feedback. So it's easily suffered by attacks from some peers that tell a lie. The other [3] [4] is to form a trust chain and use iterated algorithm to compute the degree of trust. This method needs to maintain a larger table to record every peer's trust information. Beth [5] is one of the people who researched distributed trust model in the early time. He proposed the concept that made the trust quantitative and divided the trust into two Parts: direct trust and recommended trust. And then Raman and Hailes [6] [7] proposed a trust management in P2P network based on Marsh [8] model.

In order to reduce free-riders, many researches to propose their methods [9][10] . BT is depending on Tit-for-tat [11] to reduce free-riders. And this method is just for the same file: if you give me yours, I will give you mine too. But it doesn't work in occasion when you are interested in my files, but I don't care about your files.

This thesis primarily discusses what I have done and practiced in security mechanism of P2P model. This model can properly authorize the peers and control the access to services appropriately.

3. SYSTEM COMPONENTS

3.1 Requirements of System

The security access model we assumed consists of four kinds of requirements as follows:

(1) When peers want to transmit private information, they need security tunnel to do that.
(2) Before they communicate, they need each other's identity.
(3) Most of peers want to offer service to peers that they trust or get the authorization certificate by themselves.
(4) Most of peers want to get service from peers that they trust .So it can prevent them from downloading files from hacker who spread worms and viruses.

3.2 System Structure

As illustrated in Fig.1, system structure is as follows. The top level: P2P file-sharing the applications. The middle level: Security access manager, which is consisted of Trust Model, Incentive Model, and Authorization Model. The bottom level: TLS used for encrypted transmission.

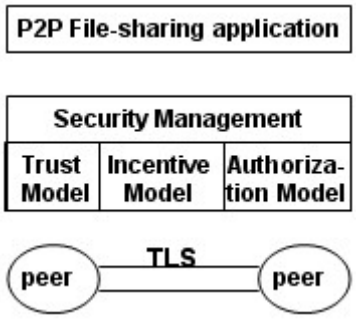


Fig.1. System Structure

3.3 Function Description

3.3.1Trust model

To tradeoff the overhead and usability, we use PGP trust model, a scalable approach that makes peers as center. It is a cumulative trust model. Peers evaluate the other peer's degree of trust using their own trust policies. There are two types of trust: direct trust and recommended trust. The degree of trust is in the [0, 1]. "0" denotes distrust; "1" denotes complete trust.

When a peer wants to get a target peer's degree of trust, he will send request to his trust peers. If his trust peers have the direct trust from the target peer, they will return the results. If not, they will continue sending the request to their trust peers, and the process goes on like that, all these recommended information will return to the requester. Finally, the requester will compute the degree of trust. As this process goes on, it establishes a web of trust. PGP uses digital signatures as its form of introduction.

In our security model, the user's ID is instead of user's public key. The visitor using provider's degree of trust determines whether his file is credible. The processing of computing the degree of trust as illustrated in Fig.2 (broken line denotes recommended trust, real line denotes direct trust)

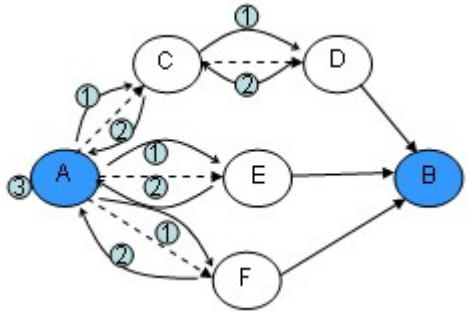


Fig.2. Computing the Degree of Trust

The following abbreviations are used in the figures.

T_{XY} : X direct trust Y;

T'_{XY} : X recommended trust Y;

Request: the request message;

Response: the response message;

SignX: X's signature.

ID_X : X's identifier.

Supposed that A wants to download B's file, he'll first compute B's degree of trust.

The process is as follows:

(1) Because A hasn't communicated with B, so he has to sent request to his neighbors for asking B's degree of trust (as illustrated in Fig.2).

$$A \to C, E, F : \mathrm{Re}\,quest[ID_A \| ID_B]$$

(2) A's neighbors will return the response with B's degree of trust.

$$C \to A : \mathrm{Re}\,sponse\{[IDK_C \| IDK_D \| T'_{CD}]_{\mathrm{si}\,gnC} + msg\}$$
$$D \to C : \mathrm{Re}\,sponse\{[IDK_D \| IDK_B \| T_{DB}]_{\mathrm{si}\,gnD} + msg\}$$
$$E \to A : \mathrm{Re}\,sponse\{[IDK_E \| IDK_B \| T_{EB}]_{\mathrm{si}\,gnE} + msg\}$$
$$F \to A : \mathrm{Re}\,sponse\{[IDK_F \| IDK_B \| T_{FB}]_{\mathrm{si}\,gnF} + msg\}$$

(3) A will list all trust chain from A to B, and multiply every degree of trust in each trust chain and sum up all and then average them.

$$T_{AB} = (T'_{AC} \bullet T'_{CD} \bullet T_{DB} + T'_{AE} \bullet T_{EB} + T'_{AF} \bullet T_{FB}) / 3$$

(4) A decides whether to access B's files according to T_{AB}.

3.3.2 Incentive Model

In many P2P network, resources are free. Therefore, a lot of free-riders appear. They just download files from other peers, while do not share their own resources. It induces the whole P2P system to reduce the usability, besides adding up futile traffic. By sampling messages on the Gnutella network over a period of 24-hours, we found out that nearly 85% of Gnutella users share no files, and nearly 50% of all responses are returned by the top 1% of sharing hosts, in 2005.

Incentive mechanism in this paper is very simple and effective. It does not only increase the usability of the system, but also solves the asymmetry in the download and upload traffic. This mechanism allocates the sharing space according to the peer's contribution .It only holds two counters: one is for upload number, it is denoted as UpNum; the other is for download number, and it is denoted as DownNum. DownNum / UpNum denote Contribution value (C) using C to estimate whether the peer is a free-rider. The peer can access resource when DownNum / UpNum $\leq$C（C=2 as a threshold and UpNum>0）if DownNum / UpNum>C(That is, download number is more than C times than upload number. They will be refused to access resources until they offer more files.)The processing is as follows:

If (T > $T_{Threshold}$)

{

If (DownNum/UpNum<C)

Access resources;

Else refuse to access;

}

Else refuse to access;

This method can discard the free-riders from P2P system effectively and encourage the node sharing to have more storage so that it can earn more reward.

In order to avoid hacker spreading bad resources, and free-riders, we propose the method using degree of trust and contribution value together to control signing the SPKI cert.

3.3.3 Authorization Model

Because of the structure of PKI is more complicated and difficult to solve access control problems. We apply SPKI to access control. The whole idea of SPKI [13] certificates is based on public key cryptography. No matter whether in generating SPKI certificates, or in using them, private keys and public keys take main roles. It has many advantages:

(1) Freedom to generate. Everyone can freely issue certificates and delegate access rights to others.

(2) Rights can be transferred. A person can delegate his rights to his trust peers.

(3) Use the public keys of entities instead of their names. SPKI avoids using globally unique names for entities.

Therefore, we can use it to define and distribute authorization freely. But it can't control re-delegating authorizations very well. In our model, we use degree of trust and contribution value to control re-delegating authorizations. The processing is as follows:

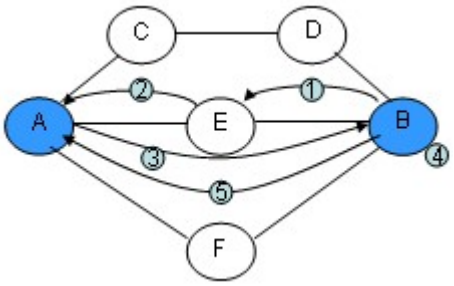


Fig.3. The Processing of Authorization

The following abbreviations are used in the figures.

$Cert_{XY}$: X signs a SPKI cert for Y;

C_X : X 's contribution value;

signX : using X's private key to sign;

K_X : X's public key;

DK_X : using K_X decrypt the message.

Supposed that A is a visitor, B is a provider for files;

The process is as follows:

(1) Because B is a provider for files, he can sign a SPKI cert for E that he trusts according to his policy.

$$B \rightarrow E : Cert_{BE}$$
$$Cert_{BE} = sign_B\{K_B \| K_E \| True \| Rights \| ValidityDay\}$$

As illustrated in Fig.4（a）.

(2) Because E obtain SPKI cert signed by B, he can re-delegate its certificates to he trust peer A. In addition, he can freely sign new certificates to A

$$E \rightarrow A : Cert_{EA}$$
$$Cert_{EA} = sign_E\{K_E \| K_A \| False \| Rights \| ValidityDay\}$$

As illustrated in Fig.4（b）.

(3) When A obtains the SPKI cert signed by C and knows B's degree of trust (the process is illustrated in 3.1), he can send an access request to B.

$$A \rightarrow B : Sign_A[msg] \| Sign_E[Cert_{EA}] \| Sign_B[Cert_{BE}] \| C_A + msg$$

(4) When B receives the request, he will do as follows:

If $C_A > C_{Thredhold}$, A will be refused. If not, B will validate the cert as follows:

$$DK_B[Cert_{BE}]_{signB} \rightarrow Cert_{BE} \rightarrow K_E$$
$$DK_E[Cert_{EA}]_{signE} \rightarrow Cert_{EA} \rightarrow K_A$$
$$DK_A[msg]_{signA} \rightarrow msg'$$
$$msg' \neq ? msg$$

if $msg' \neq msg$,A will be refused ,if not， B will merge the cert chain and compute the rights that A has(As illustrated in Fig.4（c）).

(5) B will return the result to A

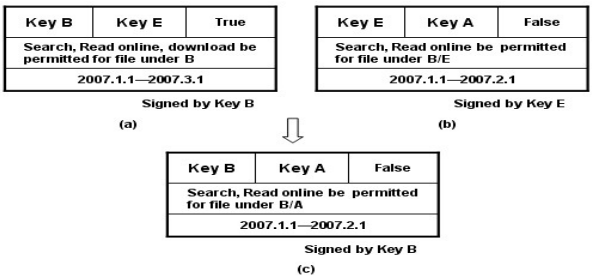


Fig.4 (a). B signs a SPKI cert for E;

Fig.4(b). E signs a SPKI cert for A.

Fig.4(c). After merged cert chain. It will create a new SPKI cert that B signs for A.

4. SYSTEM IMPLENTATION

We develop the system based on JXTA [13], and implement TLS on transmission level. Only if peer's degree of trust and contribution value reach threshold and have SPKI certificate, it can access resources.

In our P2P file-sharing system, each peer has two roles: server and client. A peer's rights are separated into three levels: search, read online, download. Fig.5 shows system flow chart.

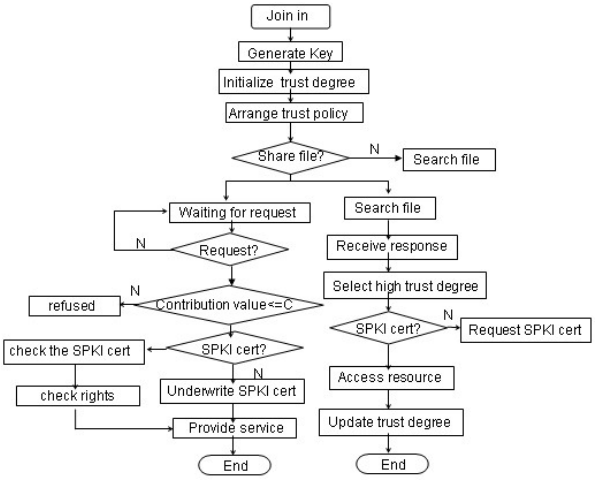


Fig.5. System Flow Chat

4.1 The Process of Peer Initialization:

(1) A newcomer has generated his own public key and private key, public key is used for identifier in the network, private key is used for proving identity during communicating with each other. Using identifier can relate trust information to a peer and accumulate history information for computing degree of trust.

(2) Because a newcomer doesn't communicate with others, so it will be given an initialization degree T, usually in a low trust level. This value approves it to have a basic right, i.e. searching files. Only after he shares his resources, he might gain more rights.

(3) Arrange its trust policy. e.g.: set threshold. If a peer that never communicate with others before, he can set a threshold a little bit low (0.4).

4.2 The Process of Peer'S Obtaining Files:

(1) To send search file request.

(2) Receive response from providers.

(3) If receive a lot of responses, select the peers that have the highest trust degree.

(4) Provider will validate the certificate, if yes turn to ⑤, if no, the peer will be refused to access.

(5) To access resources.

(6) If done, update the trust degree.

4.3 The Process of Providing Resources

① Provider will wait for other peer's access requests.

② Compare whether contribution value is less than threshold. If yes, turn to ③.If no, it will be refused to access.

③ And then validate whether the SPKI certificate is available (including digital signature, validity data, and rights), if no, the peer will be refused to access. If yes, he will communicate with the requester according to the right that he has. If a lot of peers request at the same time, select peers whose contribution value is low to priority.

5. CONCLUSIONS

In this paper, we proposed a security access model of P2P file-sharing system. PGP Trust Model can solve the malice of peer spreading bad resources; The Incentive Model can reduce free-riders; we use SPKI instead of using old ACL methods, it can be used more economically, through saving storage space and saving maintenance costs by distributing tasks to users. This model strengthens the security of P2P system.

REFERENCES

[1] eBay.http:pages.ebay.com./help/feedback/reputation-ov.html

[2] L. Mekouar, Y. Iraqi, and R. Boutaba, "A Reputation Management and Selection Advisor Schemes for Peer-to-Peer Systems", In 15*th IFIP/IEEE International Workshop on Distributed Systems: Operations & Managemen*t, CA, USA, 2004

[3] S. Kamvar, M. Schlosser, "The Eigen Trust Algorithm for Reputation Management in P2PNetworks", WWW, Budapest, Hungctry, 2003

[4] W. Dou, H. M. Wang, Y. Jia, etal. "A Recommendation-Based Peer-to-Peer Trust Modell,"in *Journal of Software*, 2004, 15(4):571583

[5] Beth T, Borcherding M, Klein B,“Valuation of Trust in Open Network[J/OL],”In *the Proceeding of the European Sysposium On Research in Computer Security (ESORICS)*,Brighton: Springer- Verlag,1994,pp3-18.

[6] Abdul-Rahman,S Hailes,“Supporting Trust in Virtual Communities[C],” In *the Proceeding of the Hawai’i International Conference on System Sciences*,pp4-7,Jan 2000.

[7] Abdul-Rahman A, Hailes S,“A Distributed Trust Model[C],”In *the Proceeding of the1997 New Security Paradigms Workshop*, Cumbria,UK:ACM Press, 1998,pp48-60.

[8] Stephen Paul Marsh,*Formalising Trust as a Computational Concept [D/OL]*. Ph.D.Thesis, University of Stirling, 1994.

[9] K. Lai, M. Feldman, I. Stoica, et.al. "Incentives for Cooperation in Peer-to-Peer Networks".in *Workshop on economics of p2p systems*, Jun 2003, Berkeley, CA.

[10] M. Feldman, K. Lai, I. Stoica, et.al. "Robust Incentive Techniques for Peer-to-Peer Networks". In *ACMElectronic Commerce*, 2004.

[11] S. Jun, and M. Ahamad. "Incentives in BitTorrent Induce Free Riding,"in *SIGCOMM 2005-Workshop on Economics of' peer-to peer systems*, Philadelphia, Pennsylvania, USA. August 22, 2005.

[12] C Ellison. SPKI *Requirements.RFC 2692*, 1999.

[13] *JXTA v2.0 Protocols Specification* http://www.jxta.org.

A Time Slices Information Concealed Cryptosystem Model

Zhichao Yan, Qingping Guo, Yifan Huang
Department of Computer Science and Technology, Wuhan University of Technology
Wuhan, Hubei 430063.P.R.China
Email: zcyan@whut.edu.cn

ABSTRACT

This paper introduces a cryptosystem model that conceals the information of time slices between the password characters. See the time-gap generated through the keystroke as cryptical information, we encrypt and decrypt it as invisible plaintext after been processed. So, in this paper there are two sets of plaintext, two sets of ciphertext, two sets of keys, two sets of encryption algorithm and decryption algorithm. It seems that the user had two locks to make the data protected more secure. And in this paper the author makes a particular analysis in extracting the time slices.

Keywords: Cryptography, Encryption, Plaintext, Time Slices, Two Locks.

1. INTRODUCTION

Along with the rapid development of the network economy, the issue of information security already became an extremely important composition in the network, but as one of the essential technologies of information security technology, cryptological technology is one of the most important tools to protect data. In the real life, the people in use of the E-mail, ATM, tools of chatting, the mobile phone, the bank card, the credit card, and so on, each aspect all needs to use the password, the password has became a inseparable thing in modern society life. However, many hackers, droved by the money or other benefits, makes some kinds of violence software to crack for the password, causes these relatively simple password ease to be cracked in a short time. Subsequently, after obtained the password they carry on to destroy the data or steal the money and so on. Either, some careless people are in order to avoid forgetting the password, they write the password in the some casual place, such as in the notebook, which could be easily discovered by the peeper, and this will cause great threat to the victim. Hundreds of thousands of passwords are stolen by others every year which causes huge loss.

Whether there is a way that even if anyone knows the other's password is "232323" and he still can not access easily? The author has designed a method which conceals the time slices between the password characters.

2. THE TIME SLICES INFORMATION CONCEALED CRYPTOSYSTEM MODEL

The cryptosystem nowadays are composed of five parts:
1) Plaintext domain M.
2) Ciphertext domain C.
3) Key domain K (Including Encryption Key K_e and Decryption Key K_d).
4) Encryption algorithm E.
5) Decryption algorithm D.

And the Sequential Cryptosystem can be represented as follows:

$M = (m_1, m_2, \cdots, m_n)$ (m_i represents single character)
$Ke = (k_{e1}, k_{e2}, \cdots, k_{en})$
$C = (c_1, c_2, \cdots, c_n)$

Thereinto:

$c_i = E(m_i, k_{ei})$ $\quad i = 1,2,\cdots,n$

Now, we add the time information to the sequential characters of Plaintext domain M:
The sequence of the characters is as Fig.1:

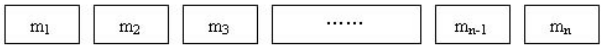


Fig.1. The sequence of the characters

Every character should have the information that contains the accurate time through striking the keyboard:

$T = (t_1, t_2, \cdots, t_n)$

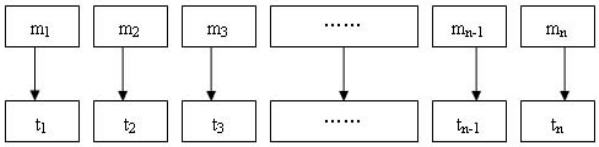


Fig.2. The record of the time of every character when striking the keyboard.

There should be a time gap y_i between t_i and t_{i+1} ($1 \leqslant i \leqslant n-1$).

$Y = (y_1, y_2, \cdots, y_{n-1})$ (Time slices domain)

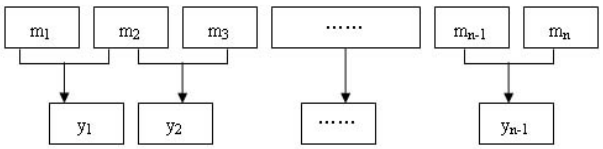


Fig.3. The time gap (time slice) generated between t_i and t_{i+1} $(1 \leqslant i \leqslant n-1)$

So, we introduce the second set of Plaintext domain Y (The time slices), the second set of Ciphertext domain $P(p_1, p_2, \cdots, p_{n-1})$, Key domain K' (composed of Encryption Key K_e' and Decryption Key K_d' and used to encrypt and decrypt the time slices domain), Encryption algorithm E', and Decryption algorithm D'.
Thus, the time slices concealed sequential cryptosystem is composed of these five parts:
1) Plaintext domain M + Plaintext domain Y
2) Ciphertext domain C.+ Ciphertext domain P
3) Key domain K + Key domain K'
4) Encryption algorithm E + Encryption algorithm E'
5)Decryption algorithm D + Decryption algorithm D'

And the new Sequential Cryptosystem can be represented as follows:

$M = (m_1, m_2, \cdots, m_n)$ $\quad Y = (y_1, y_2, \cdots, y_{n-1})$

$Ke = (k_{e1}, k_{e2}, \cdots, k_{en})$ $K'e = (k_{e1}', k_{e2}', \cdots, k_{e(n-1)}')$

$C = (c_1, c_2, \cdots, c_n)$ $P = (p_1, p_2, \cdots, p_{n-1})$

there:

$c_i = E(m_i , k_{ei})$

$p_i = E'(y_i , y_{ei}')$ i = 1,2,⋯,n

It can also be represented by the Fig.4:

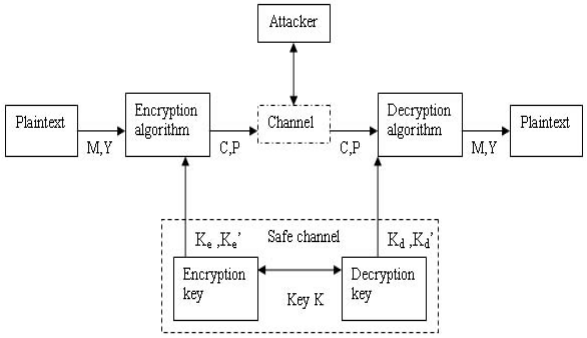


Fig.4. The time slices concealed sequential cryptosystem

In this way, we conceal the time slices information into the characters covertly according to our preestablished characters and the time information we know ourselves, and even if your password written in your notebook is peeped by someone, if he doesn't know the time information, he still can not access and obtain his intent. It's just looks like that we get two locks to make our data secure.

3. THE REPRESENT OF THE TIME SLICES DATA

step1 Search in the $Y = (y_1, y_2, \cdots, y_{n-1})$ and get the minimal value y_{min} .

step2 Sort Y ascendingly and extract the difference $Z = (z_1, z_2, \cdots, z_{n-2})$ of the neighboring time slice. Then get the minimal difference of time slice z_{min}.

step3 Compare y_{min} and z_{min} , if $y_{min} \leqslant z_{min}$, then make $Y' = (y'_1, y'_2, \cdots, y'_{n-1})$, $y'_i = y_i / y_{min}$ (y'_i is a integer that rounded up or down); Or else, $Y' = (y'_1, y'_2, \cdots, y'_{n-1})$, $y'_i = y_i / y_{min}$ (y'_i is a integer that rounded up or down).

step4 Use Y' as the second Plaintext domain, and to encrypt and to decrypt.

The flow chart of the presentation of the time slices is as Fig.5.

4. THE TIME CONCEALED CRYPTOSYSTEM MODEL AND HUMAN BEHAVIOR

(1) By this model, people could make use of the familiar and fond musical rhythm or some particular rhythm that they remember well to input the password so that they could keep their data more secure.

(2) But it's more precise when the computer calculates than people do, people cannot strike the keyboard at the very time they preestablished, so we need a stretch coefficient to process the settled time slice into an acceptable domain

For example:

Given a stretch coefficient k, for a time slice y_i, we can extend the time slice y_i to the domain $[y_i *(1-k), y_i *(1+k)]$, if $k = 10\%$, $y_i = 1.0$ *second*, all the time points are valid in that domain. It is represented as shown in Fig.6.

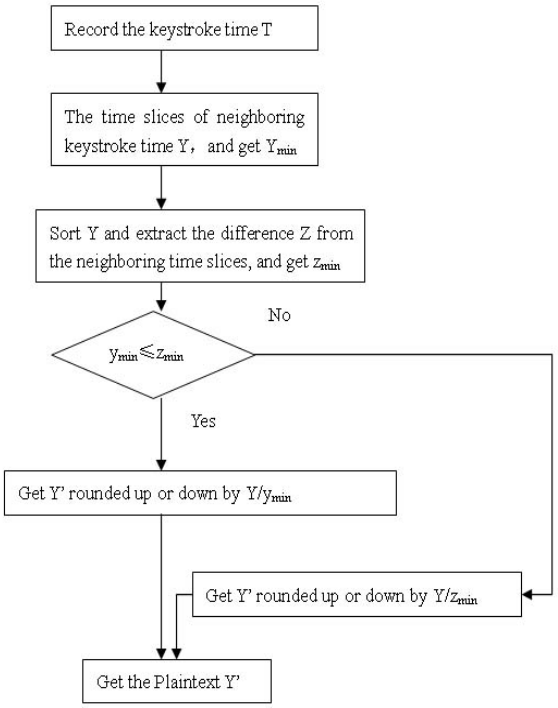


Fig.5. The flow chart of the presentation of the time slices

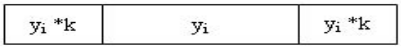


Fig.6. The extension of y_i .

(3) As the time slices concealed sequential cryptosystem needs the user has a strong manipulative ability and has a good control ability to both space and time, it's necessary for the user to have some tries before inputting the password.

5. CONCLUSIONS

The cryptosystem model that conceals the information of time slices between the password characters makes the data protected more security and hard to be cracked. The study of that model could give us more value of reference for our future study on cryptography.

REFERENCES

[1] Zhang Huanguo, Liu Yuzhen, *Introduction of cryptography*, Wuhan: Wuhan University Press, 2003.

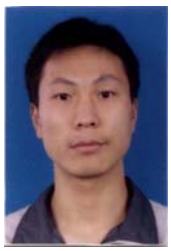
[2] Hu Xiangdong, Wei Qinfang, *Application Cryptography*, Beijing: Publishing House of Electronics Industry, 2006.

[3] Zhong Sheng, Qiu Gang, Sun Hongbin, "ID Certification Scheme Based on Time Stamp", *Journal of Computer Applications*, Vol.26, Dec 2006, pp.71~72.

[4] Li Youfa, *Numerical Calculation Method*, Beijing: High Education Press, 1996.

[5] Yang Yuhui, "The Implementation of Managing Unix

Password Based on Key of Time", *Journal of Computer Applications*, Vol.26, Dec 2006, pp.116~117.
[6] Zhu Yongjiao, "The Primality Test on Modern Cryptography", *Journal of China Science and Technology Information*, June 2006.
[7] Sun Yinglan, "Wang Xiaoyun, Making Shock to The World", *Journal of View*, October 9th 2006, pp.40~41.



Zhichao Yan is a graduate student in School of Computer Science & Technology, Wuhan University of Technology. He got his bachelor's degree in Wuhan University of Technology in 2005. His main research interests are in distributed parallel processing, network and information security.

Qingping Guo is a Full Professor and a head of Parallel Processing Lab, dean of Computer Technology Institute in School of Computer Science and Technology, Wuhan University of Technology. He graduated from Wuhan University in 1968; from Huazhong University of Science and Technology in 1981 with specialty of wireless technology. He is a holder of K. C. Wong Award of UK Royal Society (1994); was a visiting scholar of City University and University of West Minster (1986~1988), Visiting Professor of the UK Royal Society (1994), Visiting Professor of Queen Mary and Westfield College, London University (1997~2000), Visiting Professor of National University of Singapore (2000), Visiting Professor of University Greenwich (2003). He is one of the DCABES international conference founder, and will be the chairman of DCABES 2007. His research interests are in distributed parallel processing, grid computing, network security and e-commence.

Yifan Huang is a graduate student in School of Computer Science & Technology, Wuhan University of Technology. He got his bachelor's degree in Yangtze University of in 2006. His main research interests are in distributed parallel processing and cryptography.

Wireless Trust Negotiation*

Yajun Guo, Liang Wang, Huiting Wu, Huifang Yan, Mei Qi
Department of Computer Science, Huazhong Normal University
Wuhan, Hubei 430079, China
Email: ccnugyj@126.com

ABSTRACT

Trust negotiation provides a combination approach for authenticating and access control between strangers. But it is not suited for wireless network because it demands intensive cryptographic calculation and storage burden. In addition, trust negotiation is vulnerable to man-in-the-middle attacks leading to leakage of sensitive information. In this paper, we address wireless trust negotiation (WTN) to solve these problems. Credentials in wireless trust negotiation is exchanged only once, and then two parties exchanges secret key iteratively until trust negotiation succeeds or fails. WTN can avoid the heavy computational demands arising from the public key cryptography operations and needs less memory space to save credentials than those in traditional trust negotiation.

Keywords: Trust, Trust negotiation, Access control

1. INTRODUCTION

Trust negotiation[1-8] is a process of the iterative disclosure of credentials and the requests for credentials between two parties, whose goal is to establish sufficient trust so that the parties can complete a transaction. Trust negotiation relies on access control policies that govern protected sensitive resources by specifying credentials that must be submitted to obtain authorization. Credentials contain one or more attributes. Digital credentials are usually issued by the third party, and are signed by a credential issuer using its private key to testify what attributes a credential owner has. So a credential chain can be created, in which the owner of one credential is the issuer of the next credential. Access control policies govern the sensitive resources. The policy specifies which credential a party must release in order to access a specific resource. There may be some sensitive information in credentials, so one credential can be disclosed only when the access policy associated with sensitive credentials is satisfied. Each party controls the content of the message by the negotiation strategy, such as determining which credentials are disclosed, when they are disclosed and when the negotiation is halted.

Trust negotiation is not suited for wireless network because of its some weaknesses. In trust negotiation, each party must save many credentials to negotiation. If credentials don't find in the local area, searching for credentials increases excessively burdensome. Also verifying credentials and checking policy compliance is implemented by the public key which needs heavy computational demands. Man-in-the-middle attacks may occur in the process of negotiation.

2. WIRELESS TRUST NEGOTIATION

In wireless trust negotiation, each party only saves a credential including encrypted attributes. Only one credential exchanges between two parties, then iteratively disclose of secret keys to decrypt attributes and the requests for secret keys.

Digital credential in wireless trust negotiation can be implemented by using X.509 certificate. X.509v3 expands to provide binding many attributes to a credential .But attributes contained in the credential for wireless trust negotiation are encrypted. Sensitive attributes A_i in the credential are encrypted by symmetric secret key K_i , namely, $EK_i(A_i)$. Digital credentials are signed by a credential issuer using its private key and are verified by the credential issuer's public key. In order to ensure the integrity of encrypted attributes which the owner of the credential provides, the credential issuer needs to make verification process within credential as follows:

a. The credential owner use one-way function on $EK_i(A_i)$, and create fixed size digest, namely, $oneway\ (EK_i(A_i))$;

The credential owner sends $EK_i(A_i)$ to the credential issuer;

The credential issuer uses the same one-way function on $EK_i(A_i)$ to generate a digest.

The credential issuer compares the digest to the corresponding digest within the credential. If they match, the credential issuer accepts the attributes digest as the credential owner's legitimate attributes digest.

To avoid man-in-the-middle attacks, a session key must be created to encrypt message between two parties. In wireless trust negotiation, a session key is generated by oval curve secret key exchange algorithm. But the public numbers exchanging between two parties have the vulnerability of man-in-the-middle attacks. In order to prevent public numbers being instead by the third part. The secret key exchange algorithm is altered as follows:

1. $A \rightarrow B$: $C(PK_A)$
2. $B \rightarrow A$: $MAC(p_B)_{PKA}$
3. $B \rightarrow A$: $C(PK_B)$
4. $A \rightarrow B$: $MAC(p_A)_{PKB}$
5. $B \rightarrow A$: $(p_B)\ PK_A$
6. $A \rightarrow B$: $(p_A)\ PK_B$

Session key K is generated by using the secret key exchange algorithm.

7. $A \rightarrow B$: $MAC(k, 1,2,3,4,5,6)_K$
8. $B \rightarrow A$: $MAC(k, 1,2,3,4,5,6)_K$

Among them, PK_A is public key of A, and $C(PK_A)$ represents credential that contains public key of A. PK_B is public key of B, and $C(PK_B)$ represents credential that contains public key of B. p_B and p_A are respectively public numbers of B and A generated by using the secret key exchanging algorithm. The number of $1,2,3,4,5,6$ respectively represent messages that send out by step 1 to step 6.

Step 1 and step 3 send credentials that contain public key to the other party. Step 2 sends MAC for p_B, and step 4 sends MAC for p_A. Step 5 and step 6 respectively send public numbers encrypted by using public key. Because of the sequence of protocol, receiving $MAC(p_A)_{PKB}$ and $MAC(p_B)_{PKA}$ is earlier than receiving $(p_A)\ PK_B$ and $(p_B)\ PK_A$, so attackers can't modify p_A and p_B ,otherwise MAC can't match. Therefore man-in-the-middle can't generate a secret key which can

* Supported by National Natural Science Fundation of China (60403027); Natural Science Fundation of Hubei Province of China(2005ABA243).

communicate between A and B by using public numbers. Step 7 and step 8 contain *MAC* values which are all receiving and sending messages, and encrypted by new generated secret key *K*. If *MAC* values match, it can make secure communication by using new generated session key *K*.

A simple wireless trust negotiation process is as follows:

1. *A*→*B*: *A* sends a message to *B* to request service

2. Two parties generate session key *Ks* by using the secret key exchange algorithm

3. *B*→*A*: Disclose credential and service access control policy encrypted by session key *Ks* to *A*.

4. *A*→*B*: Disclose credential and service access control policy encrypted by session key *Ks* to *B*

5. *B*→*A*: Disclose secret key for a certain attribute encrypted by session key *Ks* to *A*, and *A* can decrypt the attribute value in credential by the secret key.

6. *A*→*B*: Disclose secret key for a certain attribute encrypted by session key *Ks* to *B*, and *B* can decrypt the attribute value in credential by the secret key.

…

n. *B*→*A*: Services

3. PERFORMANCES ANALYSIS

In wireless trust negotiation, the confidentiality and the integrity of attributes in credential are accomplished. Privacy of attributes can be protected and man-in-the-middle attacks are prevented in the WTN. The one-way hash function is unique because of its mathematical nature only being computable in a single direction, so attributes are integrity. Attributes in credential are encrypted by symmetric encryption, so attributes are confidential. After disclosing a symmetric secret key which can decrypt the first attribute to the other party, the other party can't know the other attribute values. The two parties can completely control the disclosure of their own attributes in credential by sending a symmetric encryption which can decrypt attributes to the other party. Thus each party can protect its sensitive attributes. In addition, during generating session key process, man-in-the-middle can't attack efficiently. WTN can prevent the vulnerability of man-in-the-middle attacks which the traditional trust negotiation has. In traditional trust negotiation, though the sensitive resources gradually disclose to the other party under protect of the access control policy, it is transparent for man-in-the-middle. At present, protecting sensitive information by trust negotiation technology is restricted in the two parties, but attackers are not restricted.

WTN needs less memory space than that of traditional trust negotiation. In the WTN, two parties save only one credential, but every party saves many credentials in the tradition trust negotiation. If credentials don't find in the local area, searching for credentials increases excessively burdensome. The difference between the size of credentials in WTN and in traditional trust negotiation is not obvious. Two kinds of credentials are implemented by using X.509v3 certificate. Generally, X.509v3 certificate is about 1000 bytes. The number of encrypted attributes in credential for WTN is possible more than that in common credential, but one credential is obviously less than several credentials.

The calculation tasks in traditional trust negotiation mainly contain verifying credentials and checking policy compliance, and probably contain searching for credentials. Verifying process is implemented by the public key which has the heavy computational demands. There exists a secret key distribution phase is in WTN, but not in traditional trust negotiation. Therefore computational demands of the WTN are more than those in traditional trust negotiation at the beginning. The overall computational demands depend on the negotiation strategy. Table 1 and table 2 give Crypto++ 5.2.1 benchmarks (Pentium 4, 2.1 GHz processor under Windows XP) timing information of several relevant cryptographic operations. From the two tables we can infer that if a eager negotiation strategy is selected, the negotiation between two parties is finished quickly. Computational demands of the traditional trust negotiation are probably less than those of the wireless trust negotiation. If using cautious negotiation strategy, computational demands of the wireless trust negotiation are usually less than those of the traditional trust negotiation. In addition, the size of message transferred between two parties in wireless trust negotiation is obviously less than that of the traditional negotiation trust.

Table 1. Crypto++ 5.2.1 cryptographic algorithm speed benchmarks

Algorithm	MB/s	Algorithm	MB/s
MD2	3.994	HAVAL (pass=3)	108.544
Md5	216.674	HAVAL (pass=4)	69.283
SHA-1	67.977	HAVAL (pass=5)	67.439
SHA-256	44.460	Rijndael (128-bit key)	61.010
SHA-512	11.392	Rijndael (192-bit key)	53.145
DES	21.340	Rijndael (256-bit key)	48.229
RC6	37.814	IDEA	18.963

Table 2. Crypto++ 5.2.1 cryptographic operation time benchmarks

Operation	Time/ms
RSA 1024 Encryption	0.18
RSA 1024 Decryption	4.77
RSA 1024 Signature	4.75
RSA 1024 Verification	0.18
LUC 1024 Encryption	0.21
LUC 1024 Decryption	7.90
LUC 1024 Signature	7.77
LUC 1024 Verification	0.21
XTR-DH 171 Key-Pair Generation	1.79
XTR-DH 171 Key Agreement	3.68
Rabin 1024 Encryption	1.66
Rabin 1024 Decryption	6.30
Rabin 1024 Signature	6.14
Rabin 1024 Verification	1.61
ECDHC over GF(p) 168 Key-Pair Generation	3.26
ECDHC over GF(p) 168 Key Agreement	3.40
DH 1024 Key-Pair Generation	2.19
DH 1024 Key Agreement	3.86

4. IMPLEMENTATION

TrustBuilder[1] can be used to implement traditional trust negotiation. It is a middleware trust agent written with Java, which can manage keys, credentials, and access policy, and can decide which credential and access policy are shown in one negotiation. In TrustBuilder, first a client sends an applying resource message to the server to request accessing resource *R*. This request triggers the trust negotiation, so the server uses a negotiation protocol named *TrustBuilder_handle_disclosure_message* to negotiate. Then the client can exchange message with the server till the resource *R* is transferred to the client or one party in the communication sends a failed message to terminate the protocol. In the structure of TrustBuilder, every party will communicate with a security agent who is in charge of the negotiation. The structure of TrustBuilder security agent comprises three parts. The first one is the credential checking module which is used to validate every received credential, verify the sign in every credential, check the credentials which may be recalled, and detect the credential chain. The second is

the policy consistency checker that will ensure the local resource can be displayed to others only when its security policy is satisfied, and can decide which local policy will be satisfied when a credential is shown. The aims of the policy consistency checker contain checking which credential from the other party can satisfy with the local policy and deciding which local credential can satisfy with the policy of the other party. The last one, the negotiation policy module can dedicate the status of the current negotiation which includes the local credential and policy, all the credentials and access polices shown in former negotiation, and the next message that will be sent to others.

To implement wireless trust negotiation, some changes must be made in the TrustBuilder.

(1) Symmetric cipher are used to encrypt the attributes of X.509v3 certification.
(2) The policy consistency checker is used to inspect if the attributes could satisfy the security policy.
(3) The access control policy should be related with the attribute level.
(4) The negotiation strategy provides access control on the attribute levels. It decides which attribute could be shown, when it will be shown and when it will be terminated.

5. CONCLUSIONS

In this paper we present wireless trust negotiation method, in which the two strangers exchange credential just only once, and then iteratively disclose the secret key. One-way function is used to verify the attributes in credential. To avoid the heavy computational demands the public key cryptography operations bring about and the vulnerability of man-in-the-middle attacks, WTN is well-suited to use resource-constrained device to secure transaction.

REFERENCES

[1] M. Winslett, T. Yu et al, “Trust Negotiation on the Web”, *IEEE Internet Computing, Vol.6, No.6, 2002*, pp. 30-37.
[2] A. Hess, J. Holt et al. *Content-Triggered Trust Negotiation, ACM Transactions on Information and System Security*, Vol.7, No.3, pp. 428 – 456.
[3] R. Bradshaw, J. Holt, K. E. Seamons, “Concealing Complex Policies with Hidden Credentials”, in *Proceedings of the Eleventh ACM Conference on Computer and Communications Security*, Washington, DC, 2004, pp.146-157.
[4] T. Ryutov, L. Zhou et al, “Adaptive Trust Negotiation and Access Control,” in Proceedings of *the 10th ACM Symposium on Access Control Models and Technologies, Stockholm*, Sweden, 2005, pp.139-146.
[5] P. A. Bonatti, D. Olmedilla, “Driving and Monitoring Provisional Trust Negotiation with Metapolicies,” in *Proceedings of the IEEE 6th International Workshop on Policies for Distributed Systems and Networks, Stockholm, Sweden, 2005*, pp.14–23.
[6] D. Xiao, J. Guo, X. Chen, “Research on A Defending Strategy for Man-in-the-Middle Attacks,” *Computer Engineering & Science, Vol.26, No.9, 2004*, pp. 7-8.
[7] K. Frikken, M. Atallah, J. Li, “Hidden Access Control Policies with Hidden Credentials,” in *Proceedings of the 3rd ACM Workshop on Privacy in the Electronic Society*. New York: ACM Press, 2004.
[8] E. Bertino, E. Ferrari , A. C. Squicciarini, “Trust-X: A Peer to Peer Framework for Trust Negotiations,” in *Proceedings of the IEEE Trans. on Knowledge and Data Engineering*. Washington: IEEE Computer Society Press, 2004.

Modelling Trust Relationships in Distributed Environments

[1]Changzheng Liu, [2]Guiyun Ye
[1]College of Computer Science and Technology, Harbin University of Science and Technology
Harbin, Hei Longjiang, 150080, P.R.China;
[2]College of Electrical and Information Engineering, Heilongjiang Institute of Science and Technology
Harbin,Hei Longjiang, 150027, P.R.China
[1]Email: fox@hrbust.edu.cn [2]Email: yeguiyun@yahoo.com.cn

ABSTRACT

Trust management and trustworthy computing are becoming increasingly significant at present. Over the recent years there have been several research works that have addressed the issue of trust management in distributed systems. However a clear and comprehensive definition that can be used to capture a range of commonly understood notions of trust is still lacking. In this paper, we give a formal definition of trust relationship with a strict mathematical structure that can not only reflect many of the commonly used extreme notions of trust but also provides a taxonomy framework where a range of useful trust relationships can be expressed and compared. Then we show how the proposed structure can be used to analyze both commonly used and some unique trust notions that arise in distributed environments. This proposed trust structure is currently being used in the development of the overall methodology of life cycle of trust relationships in distributed information systems.

Keywords: Distributed Environment, Trust Management, Trust Relationship.

1. INTRODUCTION

The concept of trust has been used and studied in social science for a long time [1, 2]. Trust was originally used in human and social issues in day-life relationships, laws, regulations and policies. In the computing world, the trust was originally used in the context of trusted computing such as trusted system, trusted hardware and trusted soft-ware [3]. Recently, trust has been used in the context of trust management in distributed computing [4–7]. When the Internet and web technologies are broadly and increasingly used in daily life for electronic commerce, trust becomes a very hot topic [8, 9]. The trust between customers and e-vendors includes not only technical aspects but also social aspects. In this paper, we will provide our definition of trust relationship. Most of the issues relating to social aspects of trust is beyond the scope of this paper, but we hope that our general definition of trust relationship can cover both aspects. The trust relationships of involved entities or computing components in distributed computing are our major concern.

XML-based Web Services technologies have been rapidly evolving since 1999. Web Services technologies address the challenges of distributed computing and B2B integration. There are huge number of service oriented applications on the Internet and they are coupled loosely. Web Services technologies target at loosely-coupled, language-neutral and platform-independent way of linking applications for business process automation within organizations, across enterprises, and across the Internet. There is no centralized control and the users are not all predetermined. Normally, the computing components involved in an e-service can belong to different security domains and there is no common trusted authority for the involved entities. How to define/model trust relationships between computing components is an important and challenging issue in the design of web services. The draft of WS-Trust was proposed in 2002 [10]. Unfortunately, the current WS-Trust only touches the issue of trusted message exchange and has not provided more details for dealing with trust relationships.

In all these trust management systems, trust and its related concepts are assumed in a specific way relating to the specific topics. There is no consensus on the definition of trust. In PolicyMaker and KeyNote, M. Blaze et al provided clear definition of trust management system and there are many clues to understand what trust is but they did not comment on the concept of trust directly. In REFEREE, Y. H. Chu et al described trust as “to trust is to undertake a potentially dangerous operation knowing that it is potentially dangerous”. Tyrone et al [11] gave a definition of trust as “the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context”. Y. H. Chu et al and Tyrone et al talked about trust in a kind of general terms, however trust is difficult to express without a strict mathematical structure. In Policy-Maker, KeyNote and REFEREE, a new trust management layer has been successfully built but the concept of trust and how to model trust has not been considered carefully. It is necessary to have a solid understanding of the concept of trust relationship and to develop a powerful set of tools to model the trust relationships for trust management in distributed information systems.

The starting point of this research is trust in the context of distributed environments. Here we have not separated the traditional distributed computing and the Web Services. Web Services are included when we talk about distributed computing for the consideration of trust issues. The rest of the paper is structured as follows. In section 2, we give the definition of trust relationship and discuss some extreme cases. In section 3, we give a series of definitions, propositions and operations about trust relationships. The mathematical properties of trust relationships are embedded in these definitions, propositions and operations. In section 4, we provide two scenario examples of trust relationships and we give some analysis of trust relationships using the definitions, propositions and operations in section 3.

2. DEFINITION OF TRUST RELATIONSHIP

Most of the researchers agree that a trust relationship is the

* This work is supported by the Natural Sciences Foundation of Heilongjiang Province under Grant QC04C44, Doctor Foundation mgb05006, Natural Sciences Foundation of China mgz06011 and the Foundation of office of Education of Heilongjiang Province under Grant 11511070.

relationship between a set of thrusters and a set of trustees in a specified context, but it is not clear enough, especially when it is used in the computing world. There is a need to convert the generally used terms into strict mathematical structure in algorithms of real systems. In this paper, we will provide our definition of trust relationship with a strict mathematical structure.

In trust management of distributed information systems, we believe that the definition of trust should have the following characteristics:

(1) The definition of trust is unique and can be used for different computing purposes.
(2) The definition of trust has strong expressive power and makes the system as simple as possible.
(3) The definition of trust has a strict mathematical structure.
(4) The definition of trust provides the solid foundation for discussing the properties of trust relationships.
(5) The definition of trust follows hard security mechanisms.

Hard security assumes complete certainty and it allows complete access or no access at all. Here we only model the static status of trust in distributed environments.

We believe that it is not enough to understand trust as a simple bilateral relation between trusters and trustees. The whole syntax of trust relationship should be "under a set of specified conditions, a set of trusters trust that a set of trustees have a set of specified properties (the set of trustees will/can perform a set of actions or have a set of attributes)". The definition is expressed as follows:

Definition 1 A trust relationship is a four-tuple T=<R,E,C,P> where:

(1) R is the set of trusters. It contains all the involved thrusters. It can not be empty.
(2) E is the set of trustees. It contains all the involved trustees. It can not be empty.
(3) C is the set of conditions. It contains all conditions (requirements) for the current trust relationship. Normally, trust relationship has some specified conditions. If there is no condition, the condition set is empty.
(4) P is the set of properties. The property set describes the actions or attributes of the trustees. It can not be empty. The property set can be divided into two sub sets: Action set: the set of actions what trusters trust that trustees will/can perform. Attribute set: the set of attributes what trusters trust that trustees have. Anywhere, a trust relationship must be used with full syntax (four-tuple <R,E,C,P >. Trust relationship T means that under the condition set C, trustier set R trust that trustee set Ehave property set P. There are some extreme cases of the trust relationship when some involved sets included nothing(empty set) or anything(whole set of possible entities).

The extreme cases have special meanings and are crucial in the understanding of the definition of trust relationship. These extreme cases will play important roles in the real world. The followings are the five extreme cases of trust relationship:

(1) R is ANY. Truster set includes all possible entities. All possible entities trust that the set of trustees Ehave the set of properties Pender the set of conditions C.
(2) E is ANY. Trustee set includes all possible entities. All possible entities can be trusted to have the set of properties P by the set of trusters R under the set of conditions C.
(3) C is EMPTY. There is no condition in the trust relationship. The set of thrusters R trust that the set of trustees E have the set of properties P without any condition.
(4) P is ANY. The property of the trustee can be anything. The set of trusters Rtrust that the set of trustees E have all possible properties under the set of conditions C.
(5) C is EMPTY and P is ANY. The set of trusters R trust that the set of trustees E have all possible properties without any condition. This case happens when the set of trusters R trust the set of trustees E by default.

When the full syntax of the trust relationship is not used, trust relationship is easily misunderstood. Normally, there are many implicit assumptions and some parts of full syntax are usually omitted. When we analyze the true meaning of a trust relationship, the full syntax must be recovered. Our definition of the trust relationship has strict mathematical structure with the full syntax in any case. There is no confusion when the full syntax trust relationship is used in any information system.

It is straightforward to use the set of conditions in the definition of trust relationship. When a trust relationship is used, trusters, trustees and properties are normally involved individually. The trust relationship can always be evaluated based on one truster, one trustee and one property. In our definition of trust relationship, the trusters, trustees and properties turn up as sets are based on the following concerns

(1)The concept of security domain is broadly used and related technologies are quite mature. The role-based access control is broadly used and well understood by programmers and business people. When a set of trusters, a set of trustees and a set of properties are used in the definition of trust relationship, the similar ideas in security domain and role-based access control can be employed easily. It is convenient to define some abstraction characteristics based on a group of trusters, a group of trustees and a group of properties. We hope that a set of trusters, a set of trustees and a set of properties in the definition of the trust relationship have better abstraction and it is easier to use the definition. (2) The set theory can provide formal mathematical notion and handy tools to discuss the relationships of sets. (3) An individual truster (or trustee, or property) is a special case of the set of trusters (or trustees, or properties). (4) It is convenient to discuss special cases of trust relationship when truster (or trustee, or property) is anyone.

3. MATHEMATICAL PROPERTIES

In this paper, we will discuss the mathematical properties of trust relationship based on our strict definition of trust relationship. The trust relationship has a full syntax with truster set, trustee set, condition set and property set. It is incorrect to only talk about the trust relationship between trusters and trustees without mention of the condition set and property set. The discussions of properties of trust relationship should be based on the full syntax of trust relationship in its definition. In the following part of this section, we will give some definitions, propositions and operations related to trust relationships. The mathematical properties of trust relationships are embedded in these definitions, propositions and operations. These mathematical properties focus on some relations of trust relationships and they will be used as tools in the analysis and design of trust relationships in real systems.

From the nature of trust relationship and its mathematical structure, some new trust relationships can be derived based on the existing trust relationships. In the follows, we will define the operations of using two existing trust relationships to generate a new trust relationship under specific constraints and operations of decomposing one existing trust relationship into two new trust relationships under specific constraints.

In the following part of this section, we will focus on the relation of trust relation-ships, especially we will discuss and define the equivalent, primitive, derived, direct redundant and alternate trust relationships. We will classify the direct redundant trust relationships into different types as well.
Definition 2 Let T1 =<R1,E1,C1,P1 >and T2 =<R2,E2,C2, P2 >. If and only if R1 = R2 and E1 = E2 and C1 = C2 and P1 = P2,then T1 and T2 are equivalent, in symbols:
T1 = T2 R1 = R2 andE1 = E2 and C1 = C2 and P1 = P2
Definition 3 If a trust relationship can not be derived from other existing trust relationships, the trust relationship is a primitive trust relationship.
Definition 4 If a trust relationship can be derived from other existing trust relation-ships, the trust relationship is a derived trust relationship.

Note: Trust relationships are predefined in information systems. A derived trust relationship is always related to one or more other trust relationships. For an independent trust relationship, it is meaningless to judge it as a derived trust relationship or not. Proposition 1 If a derived trust relationship exists, there is information redundancy. Proof. When the derived trust relationship is moved out of the system, the information of the derived trust relationship has not been lost. The derived trust relationship can be built when it is necessary. From the view point of information, there is redundancy. A DMC-redundant trust relationship may have multiple alternate trust relationships with different sets of non-redundant conditions.

4. TRUST RELATIONSHIPS

In this section, we make up two scenarios for discussing trust relationships in the real world. We hope that these examples can be helpful in understanding the definition of trust relationship and mathematical properties of trust relationships expressed in section 2and section3.

Scenario 1: When people want to change their names, they need to apply to a spe-cific organization (In Australia, the organization is the Registry of Birth Deaths & Mar-riages). The officers in the organization and the requesters are involved in this scenario.

Scenario 2: An online e-commerce service is called FlightServ which can provide flight booking and travel deals. FlightServ is designed based on the new technologies of web services. FlightServ connects with customers, airlines, hotels and credit card services (some of them maybe web services). The whole system could be very complicated, but we only consider some of trust relationships in the system. In the system, customers are classified into normal flyers and frequent flyers. Originally, some trust relationships are modeled as:
TS2-1 Airlines trust normal flyers if they have address details & confirmed credit card information that normal flyers can make their airline bookings.
TS2-2 Airlines trust frequent flyers with no condition that frequent flyers can make their airline bookings.
TS2-3 Hotels trust normal flyers if they have address details & confirmed credit card information that normal flyers can make their hotels booking.
TS2-4 Hotels trust frequent fllyers if they have address details & confirmed credit card information that frequent flyers can make their hotels booking.
TS2-5 Credit card services are trusted by all possible entities without any condition that the credit card services will give the correct evaluation of credit card information.
TS2-6 Credit card services are trusted by all possible entities without any condition that the credit card services will keep the privacy of credit card information.

For the above trust relationships in the system, based on definitions and operations in section 3, we have the following analysis:

(1) All above trust relationships are primitive.
Using the Operation 3A, trust relationships TS2-3 and TS2-4 can be merged to a new trust relationship TS2-(3)(4): “Hotels trust customers if they have address details & confirmed credit card information that customers can make their hotels booking”. If TS2-(3)(4) has been defined in the system, TS2-3 and TS2-4 becomes DLE-redundant trust relationships and will be removed out of the system.

(2) Using the Operation 1B, trust relationships TS2-5 and TS2-6 can be merged to a new trust relationship TS2-(5)(6): “Credit card services are trusted by all possible entities without any condition that the credit card services will give the correct evaluation of credit card information & the credit card services will keep the privacy of credit card information”. If TS2-(5)(6) has been defined in the system, TS2-5 and TS2-6 becomes DLP-redundant trust relationships and will be removed out of the system.

Obviously, the definition of trust relationship in section 2 and the mathematical properties of trust relationships in section 3 provide terminologies and helpful tools in the analysis of the two scenarios. In the analysis of the two scenarios, we only employ some definitions, propositions and operations expressed in section 3. We hope that these examples can provide a general picture for the usage of the definitions, propositions and operations. In these two scenarios, we only choose some trust relationships as examples and there are more trust relationships. The systematic methodologies and strategies for modeling trust relationships are beyond the scope of this paper as well and will be discussed elsewhere.

5. CONCLUSIONS

The definition of the trust relationship provided in this paper has a strict mathematical structure and broad expressive power. The definition is suitable for any computing purpose. The mathematical properties of trust relationships are shown in a series of definitions, propositions and operations. We believe that these definitions and mathematical properties of trust relationships provide useful tools for enabling the analysis, design and implementation of trust in distributed environments. This research only provides a starting point for the analysis and design of trust relationships in distributed information systems. How to model trust relationships in distributed information systems and how to merge the trust relationships into the over-all distributed information systems provides lots of challenges for further research. We believe that our definition of trust

relationship and the associated mathematical proper-ties described in section 3 could be used as helpful tools to model the trust relationships. The definitions and operations in section 3 provide some starting points and tools for the analysis and design of the trust relationships in a system. We are currently working on using the proposed definition of trust relationship and mathematical properties of trust relationships to develop a methodology for modeling trust in distributed systems. This involves several stages such as extracting trust requirements in system, identifying possible trust relationships from trust requirements, choosing the whole set of trust relationships from possible trust relationships and implementing and maintaining trust relationships in systems. We will describe them in details in a separate paper.

REFERENCES

[1] M. Deutsch, "Cooperation and trust:some theoretical notes", Nebraska Symposium on Mo-tivation, Nebraska University Press, 1962.

[2] D. Gambetta, "Can we trust trust?" In *Trust:Making and Breaking Cooperative Relations*, Basil Blackwell, Oxford, pp.213-237, 1990.

[3] J. Landauer, T. Redmond *et al*. "Formal policies for trusted processes", *Proceedings of the Computer Security Foundations Workshop II*, 1989.

[4] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management", *Proceedings of the IEEE Conference on Security and Privacy*, Oakland, 1996.

[5] M. Blaze, J. Feigenbaum, and J. Lacy, "KeyNote:Trust management for public-key infras-tructure", *LNCS 1550*, pp.59-63, 1999.

[6] KeyNote web page, "The KeyNote Trust-Management System",http://www.cis.upenn.edu/ keynote/.

[7] Y. H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick and M. Strauss, "REFEREE:Trust Management for Web Applications", *AT&T Research Labs*, 1997, http://www.research.att.com/ mstraus/pubs/referee.html.

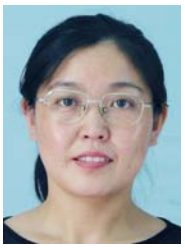
[8] A. Kini and J. Choobineh, "Trust in electronic commerce:defintion and theoretical consider-ations", *31st Annal Hawaii International Conference of System Sciences*, Hawaii, 1998.

[9] D. W. Manchala,"Trust metrics, models and protocols for electronic commerce transac-tions", *Proceedings of 18th International Conference on Distributed Computing Systems*, 1998.

[10] G. Della-Libera et al, "Web Services Trust Language (WS-Trust)", http://www-106.ibm.com/developerworks/library/ws-trust/, December 18th, 2002.

[11] T. Grandison and M. Sloman, "A survey of trust in Internet application", *IEEE Communica-tions Surveys*, Fourth Quarter, 2000.

Changzheng Liu is a vice Professor of Computer Science and Technology College, Harbin University of Science and Technology. He graduated from Harbin Engineering University in 1993; was a postdoctor of Harbin Medical University (2004~2006). He is secretary-general of Hei Longjiang Biomedical Engineering Society. He has published over 20 Journal papers. His research interests are in distributed parallel processing, Visualization in Scientific Computing



Guiyun Ye is a vice Professor of College of Electrical and Information Engineering, Heilongjiang Institute of Science and Technology, She graduated from Harbin Engineering University in 1986. She has published over 30 Journal papers. Her research interests are in distributed parallel processing, Visualization in Scientific Computing.

Research and Implementation of User Identification Methods of IP DSLAM

Chuanqing Cheng [1], Li Wang [2]
[1]Computer Science Department, Wuhan University of Science and Engineering
[2]School of Telecommunication, Wuhan University
Email: ccqcjl2005@126.com

ABSTRACT

A very important reason of hostility attack flooding in internet is that there is little traceability mechanism. In most cases the person who have behave maliciously will not be found and to be punished, so the network attack is coming in thick and fast.The traceability technology is very important to improve the network security. If the attacker is easy to be found, the insecurity will prevent him from attacking network to a certain degree. For example, there is few DDoS attack in PSTN because its traceability mechanism. The key technology is to realize the physical location of attacker and traceability on different layer. This paper introduces some methods of traceability and discussed the implementation of traceability scheme.

Keywords: Switch User-Identification DHCP PPPoE VLAN

1. INTRODUCTION

IP network is generated for military affairs and research, which is aimed to unreliable transmitting path and to realize end to end packet transmitting. The application of the packet switch network is nonprofit. Based on it, some eidos, just as simple, open, end-to-end transparent character, user-self-discipline, fairness, are the core character of packet switch network.

On one hand, because of these eidos, the network has spread all of the world and applied widely .But because of these eidos at the other hand, it is negative for network security. Even to be said, the security challenge of current IP network is leaded by these eidos

The IP network is for research at the beginning, so the user is reliable to each other. The design of network security guarantee is based on user-self-discipline. The main task of IP network is to improve performance and work in new application and not is the security. Because presuming the user is reliable, there is not any check scheme in network or protocol design. No authentication, no traceability, no award and no punishment. When the IP network is extended to be internet, and used for business, the user is not reliable, so the network security becomes a great problem.

A very important reason of hostility attack flooding in internet is that there is little Traceability mechanism. In most cases the person who has behaved maliciously will not be found and to be punished, so the network attack is coming in thick and fast. The traceability technology is very important to improve the network security. If the attacker is easy to be found, the insecurity will prevent him from attacking network to a certain degree. For example, there is few DDoS attack in PSTN because its traceability mechanism. The key technology is to realize the physical location of attacker and traceability on different layer.

So the methods to implement user- identification and traceability are very important to the high speed IP switch network. Some methods of traceability are in dire need to get user information.

The section2 will introduce some methods of traceability. The implementation is discussed in section 3.Section 4 is the conclusion of this paper.

2. METHODS Of USER IDENTIFICATION

On the development of broadband network, there are some traceability methods such as DHCP Option82, VBAS, PPPoE+, Stack VLAN. In the main, when the user logins in the system, the DSLAM report the user physical information to BRAS according to the pre-determined. protocol format.

DHCP option82 is a method to implement user identification and traceability by adding special user-identification field in the DHCP packet via DHCP agent. PPPoE+ is the abbreviation of PPPoE Intermediate agent. The method is put forward in DSL forum firstly. It is defined just as RFC 3046. The two methods is the supplement of original protocol and can be conveniently implemented to realize bind of user name, IP address, user port. It can improve user management to mark user but not mark service.

Beside of these methods, VLAN(stacking VLAN), VBAS, VMAC are the often-used methods to implement traceability.

2.1 PPPoE Plus

PPPoE+ is recommended by DSL forum as a solution to DSLAM user- identification and traceability aimed to standard PPPoE protocol. The core thought is to extend the PPPoE protocol, use the “Tag Type” field to mark user’s physical port information, which is ignored in standard PPPoE protocol. The PPPoE+ is easy to implemented .Only by upgrading software, can implement it and can protect current device investment.

For the PPPoE discovery packet, there is one or more Tag in the payload. The Tag type field in PPPoE is not defined in detail as in PPP. So it can be used in PPPoE+.The format of the tag type is like the Table 1:

Table 1. Tag of PPPoE

type	lenth
data	

Fig.1 is the PPPoE+ protocol. On the PPPoE discovery stage, when host send unicast request to server(PADR packet),it add line ID information to PADRpacket by fill Tag Type fiel

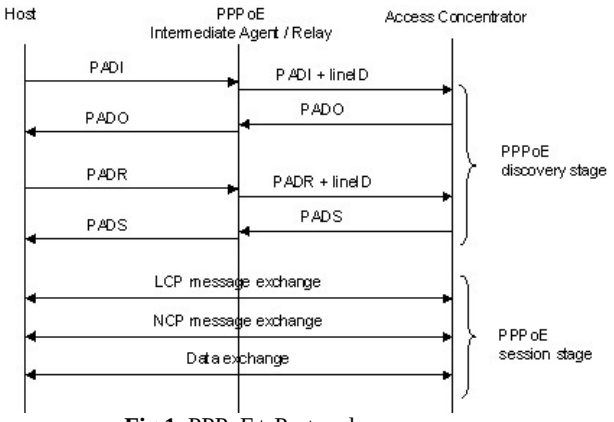


Fig.1. PPPoE+ Protocol

2.2 DHCP OPTION82

DHCP Option82(RFC3046) is recommended by DSL forum, which is aimed to DHCP+WEB authentication way to implement traceability. The main problem of DHCP authentication is to assure DCHP access security. On the DHCP setup stage, DSLAM insert the user physical port information to DHCP discovery message and transmit it to BRAS.DHCP option82 is a the supplement of original protocol based on DHCP. The access node (DSLAM) captures the DHCP protocol packets on both upstream and downstream direction as a layer2 DHCP relay agent. DHCP option82 inserts the user port information to Option82 field in upstream direction and peels off it in downstream direction. DHCP server implement IP designate policy or other policy by recognizing the Option82 filed.

Figure2 is DHCP Option82 protocol.

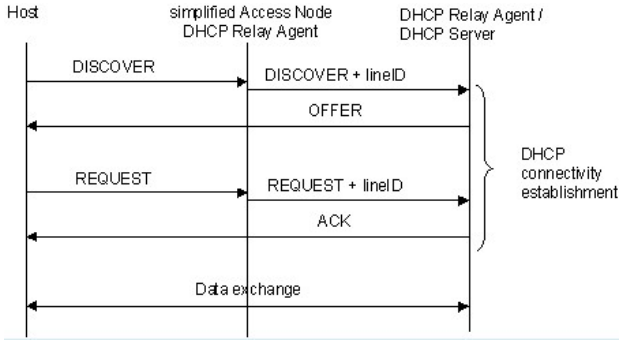


Fig.2. DHCP Option82 Protocol.

2.3. VLAN Stacking

In fact, for packet switch network device like IP DSLAM, the basal user-identification and traceability method is to assign different VLAN ID to different user. As long as every user has a exclusive VLAN ID, the user-identification and traceability is easy to be done. But the limit of VLAN ID limits the methods at the same. When the user amount of a BRAS port is exceed 4096, it is impossible to mark user by VLAN ID.VLAN stacking can extend VLAN, support 4096*4096 VLAN ID. The amount is so big to assure every user has a exclusive VLAN ID. DSLAM , LAN switch and MSTP device add internal VLAN tag for user and converge switch which connect to BRAS use VLAN stacking, and add an external VLAN ID to different DSLAM device,LAN switch or MSTP device.

2.4 VBAS

VBAS is not a BAS device, but only a protocol standard. It defines a method to exchange broadband user access port information between BRAS and IP DSLAM. When the user logins in the system to authentication, VBAS add a exchange process between BRAS and DSLAM to request user identification. When PPPoE authentication is used, the MAC address will be known by BAS. It is not sufficient for MAC address to mark a user because the MAC can be changed. For IP DSLAM, since it is Ethernet switch, it is easy to get ADSL port information by fdb, so BAS can get the user identification by request DSLAM. The figure3 is the protocol:

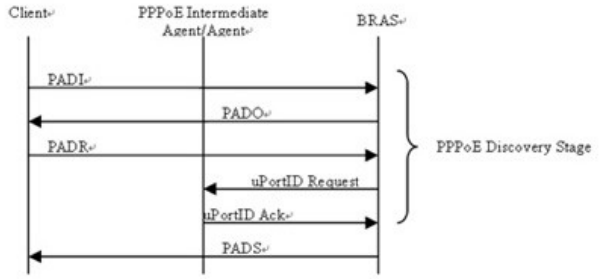


Fig.3. VBAS Protocol

2.5 VMAC

The main principle of VMAC is to transfer the MAC in Ethernet packet to a virtual MAC address and exchange user information between DSLAM and BRAS by virtual MAC address. The VMAC only exist between DSLAM and BRAS and have not influence on layer2 protocol and multicast protocol. VMAC transfer the source MAC address of upstream frame to be a frame whose source address is a VMAC. The VMAC brings the port information to BAS and RADIUS. On the downstream direction, VMAC transfer the virtual destination MAC address to original MAC address. From these steps, we can see that the RADIUS can get user information by the VMAC and can traceability easily.

3. IMPLEMENT SCHEME

The current IP DSLAM is the master-slave device, which is composed of core card which is responsible for core switch and the service card(line card), which is responsible for service access. The main structure is like Figure 4:

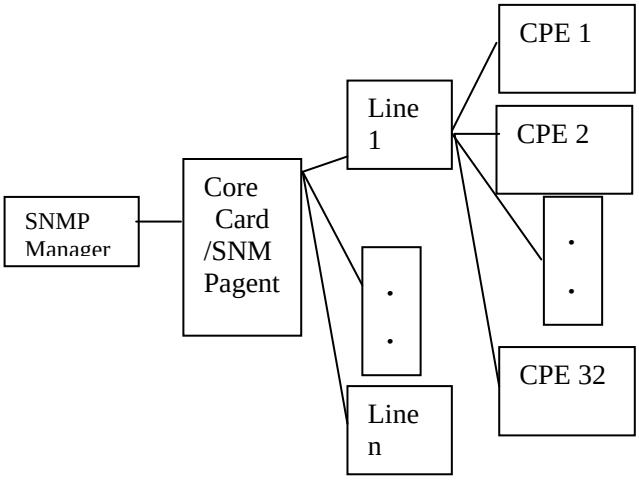


Fig.4. IP DSLAM Structure

It is obviously that it can not support user-identification and traceability function efficiently only by core card, core card

and service card must collaborative work to realize these methods. The scheme is like these:

- Service card must set filter rule to trap the special packet to CPU, such as PPPoE packet and DHCP packet.
- When service card received the authentication packet, it put it to buffer for future process instead of sending it to core card.
- Edit a special packet to core card, which include the user MAC address, slot ID, and port ID.
- Send the authentication packet which have been put to buffer to core card ;
- Core card receive the special packet and trap it to CPU.
- Core card parse the packet and extract the information to maintain the CPU address table.
- Core card to do the user-identification and traceability process as described in section2 (DHCP Option82, PPPoE+ or VBAS,VMAC).
- The processed packet is sent to upstream device (BRAS/RADIUS) to finish the authentication process.

Table 2 is the format of the special packet.

Table 2. special packet between core card and service card

Destination MAC	Source MAC	Protocol type	payload
6 bytes	6bytes	2 bytes	8 bytes

Destination MAC(6 bytes)：MAC address of core card；
Souce MAC (6 bytes):MAC address of service card.
Protocol type(6 bytes): a fixed value
Payload(8bytes): the user MAC address(6tytes)+slot(1byte)+port(1byte)

4. CONCLUSIONS

Broadband user-identification and traceability is a important question in high speed packet switch network. The technology is not applied for ADSL ,but also for LAN and VDSL. Now the telecommunication service provider Appreciate different kinds of user-identification and traceability methods and test access device for several times. It is a hot question of broadband network security. On the conclusion the final method will be the stacking VLAN to solve the problem ,but the other methods is now more practical to protect the current device investment.

REFERENCES

[1] T. Bostoen, P. Boets, M. Zekri, L. Van Biesen, T. Pollet, and D. Rabijns,"Estimation of the transfer function of a subscriber loop by meansof a one-port scattering parameter measurement at the central office,"*IEEE J. Sel. Areas Commun.*, vol. 20, no. 5, pp. 936–948, Jun. 2002.

[2] T. Chen and B. A. Francis, Optimal Sampled-Data Control Systems.London, U.K.: Springer, 1995.

[3] J. W. Cook, "The noise and crosstalk environment for ADSL and VDSL systems," *IEEE Commun. Mag.*, vol. 37, no. 5, pp. 73–78, May 1999.

[4] F. Ding and T. Chen, "Parameter estimation for dual-rate systems with finite measurement data," Dyn. Continuous, Discr. Impulsive Syst., Ser.B: Appl. Algorithms, vol. 11, no. 1, pp. 101–121, Jan. 2004.

[5] F. Ding, Y. Shi, and T. Chen, "Gradient-based identification algorithms for Hammerstein nonlinearARMAXmodels," Nonlinear Dyn., vol. 45,no. 1-2, pp. 31–43, Jul. 2006.

[6] http://ip.chinalabs.com/iptv/display/135629.html Internet security analysis and solution

[7] RFC 3046 "DHCP Relay Agent Information Option "

Chuanqing Cheng is a lecture of Wuhan University of Science Technology. He graduated from Wuhan University in 1996; with specialty of electronics and information system. He has published one bookes, over 10 journal papers and many o f which is indexed by EI or ,ISTP. His research interests are in distributed parallel processing, grid computing, network security and e-commence.

The Implementation of Cross-Domain SSO Based on Distributed Authentication*

Nie Li, Jiguang Lu
College of Computer Science, South-Central University for Nationalities
Wuhan, Hubei, 430074, PR China
Email: ljg0101@126.com, dumplingking@163.com

ABSTRACT

With the development of application systems, the burden on the single authentication server becomes heavier than ever before and the security of the system becomes worse. Distributed authentication can not only deal with this problem, but also assemble the existing application systems. In order to assemble the existing multi-authentication systems and achieve Single Sign-On (SSO) on them, it's necessary to combine the distributed authentication and SSO technology. This article has improved a cross-domain SSO system based on distributed authentication.

Keywords: Distributed Authentication, Single Sign-On (SSO), SAML, Cross-Domain, Web Service

1. INTRODUCTION

Authentication plays an important role in the requirements of information security. The traditional system based on single identity authentication server has advantages of low design and administration cost. However with the rapid development of information technology, application systems become more and more complex, the burden on the single identity authentication server becomes heavier, and the system's security becomes worse. Once the authentication server was attacked, the entire system would be collapsed. Distributed authentication server system consists of a number of authentication servers which work together to complete the whole authentication task, and improve the performance and security of the authentication system [1].

2. AUTHENTICATION AND DISTRIBUTED AUTHENTICATION

Encryption and authentication are two key technologies to achieve information security. Authentication technology is mainly for information certification, confirming the identity of senders, preventing invaders from faking legal status, and verifying the integrity of the information, which means the information isn't altered in the process of transmission and store. Authentication is also known as the identification technology which is an important technology preventing illegal persons from attacking the system. Certification includes two main aspects:

1) Entity certification: verifying whether the sender of the information is true and preventing impersonation, including the authentication and identification on the receiving party and sending party of the message.

2) Message certification: verifying the integrity of the message, validating the data isn't altered, replaced or delayed in the process of transmission and store.

Authentication technology mainly includes two aspects, information and identity authentication. Information authentication ensures the integrity and undeniable feature of the information (the undeniable feature means user can't deny his behavior later). Identity authentication is to verify the identity of the user, limit illegal access to network resources. Common identity authentication technologies include password, PKI, Kerberos and so on.

There are many security risks in the single authentication server. In a distributed authentication mechanism the process of authentication which is different from that of single authentication is carried out not only by single authentication server, but a number of cooperative servers.

There are two or more authentication servers in the distributed authentication architecture. These servers may be in the same domain or may belong to different domains and may have different product architecture. The authentication servers through standard communication protocols exchange authentication information and achieve a higher level SSO.

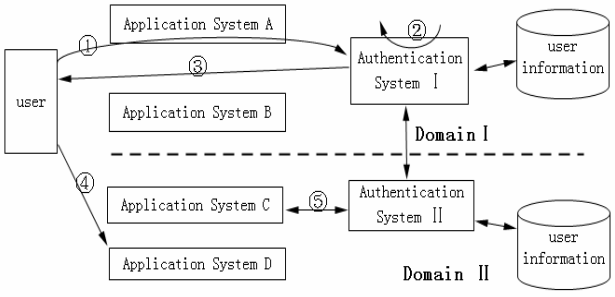


Fig. 1. Distributed authentication system

Fig.1 is a common distributed authentication architecture. A user has signed on the authentication system I when he wanted to visit the application system A in domain I (①, ②). He got a related key(③). When he wants to visit application system D in domain II later (④), the authentication system II in domain II should identify the user's identity and authority by the user's key got in Domain I(⑤).

3. OVERVIEW OF SINGLE SIGN-ON

Single Sign-On (SSO) assembles management of users' information for all unified application systems in order to achieve unified identity authentication. Once the user has signed on an authentication server, he can access all the needed application systems.

In common SSO model a single authentication server serves

* Supported by the Project " A Study on Key Technologies of Intranet"(MZY00005), Sponsored by the Fund of Natural Science, The State Ethnic Affairs Commission of PR China
Corresponding Author: Jiguang Lu

several application systems. A trusted platform is built for the application servers. Users need to sign on just for one time and then could visit all the mutual trusted application servers seamlessly. The security of this module is good and visit among servers of different domains can be achieved. But this model isn't suitable for complicated multi-authentication systems. A model of cross-domain SSO based on distributed authentication system is proposed in this paper. The combination of distributed authentication system and SSO can deal with the complex cross-domain SSO and assemble the existing SSO systems, lighten the burden on single authentication server.

Generally speaking, there are two forms of SSO: SSO based on ticket and SSO based on Web Service.

3.1 Distributed Authentication SSO Based on Ticket

The principle of authentication model based on ticket lies in that the server sends the ticket to legitimate users. Traditional application of this model is Kerberos system. The key to realize distributed authentication system based on Kerberos is to establish an authentication mechanism among the domains. A specific method is that each pair of interpretational Kerberos servers shares one secret key and registers mutually.

But the expense of Kerberos system under B/S architecture is too high. It's required that all the J2EE application systems and authentication servers to be designed according to Kerberos architecture. Further more ticket distributors are to be installed and maintained. What's more, the expansibility of this model of multi-domain is not good. The number of times of interaction of the secure secret keys will increase rapidly while the number of domains is increasing. If there are N domains, the secure secret keys must be interacted N(N-1)/2 times [2].

3.2 Distributed Authentication SSO Based on Web Service

Authentication model based on Web Service uses a Web Service as a portal, verifying the identity of all the applications. A user has only one user name and password. The key to achieve distributed authentication is to establish trusted mechanism among multiple Web Services. Commonly used Web Services include WebLogic, Apache, and Tomcat.

2.3 Cross-Domain SSO

With the increase of applications, application servers may belong to the same domain or different domains. Cross-domain is necessary for the implementation of SSO. The common model of cross-domain SSO consists of a single SSO authentication server and multiple application servers which belong to different domains. Authentication server can be located in a domain which any one of application servers belongs to. Application servers in different domains need to establish a trusted platform so that a user can visit the application systems seamlessly after he signed on.

In fact the situation is that the existing systems have their own authentications, how to assemble these systems and implement SSO? The key is to establish a distributed authentication structure from these authentication systems which are in different domains. Research and implementation of such structure are given below.

4. THE IMPLEMENTATION OF A DISTRIBUTED AUTHENTICATION SSO SYSTEM BASED ON SAML

Security Assertion Marking Language (SAML) as a description language based on XML is good for cross-domain [3]. SAML provides only standard authentication and authorization decision-making mechanism. There are no common rules about how to authenticate and authorize. SAML has multiple flexible interfaces for expansibility. As the security feature SAML takes some secure policies to cope with common attacking measures, such as Artifact theft, denial of service attacks, eavesdropping, tampering with the news, replay attacks, middleman attacks and so on. At present, the open standard SAML 2.0 has provided an entire cross-domain framework for SSO and secure authentication in Web module.

4.1 Research and Implementation of Cross-Domain SSO Based on Distributed Authentication

In order to bring about cross-domain SSO a big trusted platform of secure domains from different DNS is established. The secure domains located in this trusted platform use secret keys to establish trust relationship. Each secure domain has its own authentication server and several application servers. A user owns a corresponding identity in his own domain, but must have a unified identity in federation environment. This identity is called federation identity, which can be identified by each cooperative domain.

A SAML authentication agent module is added, which is responsible for verifying the requests of assertion carried by users in current domain. The model judges and deals with the requests of assertion carried by users in other domains, then sends them to the authentication system of their own domain for certification. This module can distinguish the assertions whether from the current domain or from other domains, achieve SSO in current domain, avoid sending all the requests to authentication system, and lighten the burden on authentication system.

The main idea of the module lies in the following: an identity federation module is established in each domain, the authentication policy mechanism is based on federation, the SAML assertions can be transferred among domains which have established the trusted mechanism, including identity and authorization. The Web Service responsible for authentication is WebLogic 8.0.

The system includes the following components:

1) Authentication system for identity: SSO Authentication Module for Identity (SSOAMI), Authentication and Authorization Module (AAM), Identity Federation Module (IFM), Storage Module for User Information (SMUI).
2) Web application system: Sign-On Control and Authorization Module (SOCAM), SAML Authentication Agent Module (SAAM).
3) Storage system for user information: Database Server.

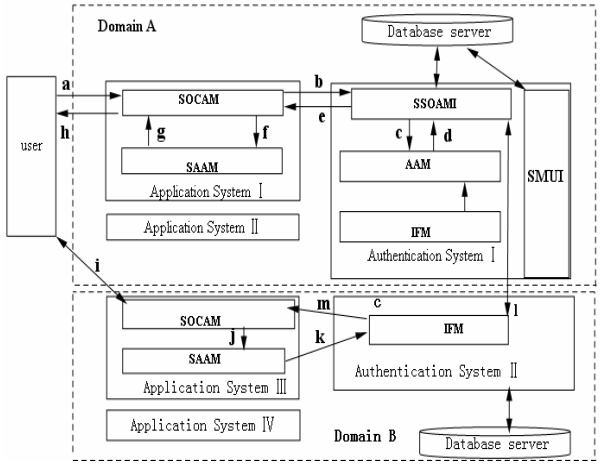


Fig.2. Cross-domain SSO based on distributed authentication

SOCAM: Sign-On Control and Authentication Module
SAAM: SAML Authentication Agent Module
SSOAMI: Single Sign-On Authentication Module for Identigy
AAM: Authentication and Authorization Module
SMUI: Storage Module for User Information
IFM: Identity Federation Module

4.2 SSO Process Based on Distributed Authentication

1) The user signs on initially in current domain

a. The user visits the Web page of application system I. The request is intercepted by SOCAM.

b. SOCAM judges whether the user has signed on or not, sends a sign-on Web page to the user if he hasn't signed on.

c. Authentication information sending by the user is intercepted by SSOAMI which sends the request to AAM.

d. AAM verifies user's identity by the database information and sends the result to SSOAMI.

e. SSOAMI judges the result, redirects the initial application Web page with assertion to the user if the authentication succeeded.

h. Application system I verifies the validity of the assertion (f, g), responds to the requested page of the user if succeeded.

2) The user has signed on in current domain

f. The user visits the Web page of application system I. The request is intercepted by SOCAM. The module sends the authentication assertion to SAAM after it has confirmed the user has signed on already.

g. SAAM verifies the validity of the assertion, sends the result to SOCAM.

h. If the result implies the authentication is successful, the user can visit the Web page.

3) The user has signed on in other domains

i. The user in domain A wants to visit the Web page of application III in domain B.

j. The request is intercepted by SOCAM. The module sends the authentication assertion to SAAM after it has confirmed the user has signed on.

k. SAAM verifies the validity of the assertion. After verifying SAAM knows the user is from authentication system I in domain A and sends the assertion to IFM in domain B.

l. IFM in domain B sends the assertion to SSOAMI of authentication system I for certification. If the authentication is succeeded, IFM in domain B inquiries the attributes of users in domain B. If there is a user in domain B who has the same attributes as the current user in domain A has, the latter obtains the same assertion as the former. Conversely the latter can obtain an assertion of identity of an anonymous user in domain B. The initial application Web page the user wants to visit will be redirected to the user along with an assertion of successful authentication.

m. Application III judges the validity of the assertion and responds to the requested Web page if the assertion is valid.

5. CONCLUSIONS

The combination of distributed authentication and SSO technology can deal with the problem of multi-authentication system on cross-domain SSO, achieve sharing resources, and lighten the burden on authentication system. The key of distributed authentication system is security. SAML is a secure descriptive language based on XML, and well suit for cross-domain. A cross-domain SSO mechanism is implemented on distributed authentication system based on SAML and identity federation in this paper.

REFERENCES

[1] Liu Rui-yang, "Distributed Certification System on A Trusted Dealer and Secure Interactions," *Ph.D. Dissertation*, Zhejiang University, PR China, May, 2003, pp.38~60

[2] William Stallings, "Cryptography and Network Security: Principles and Practices," *Third Edition, Pearson Education*, Inc., 2003, pp.410

[3] Hal Lockhart, Nick Ragouzis, *Security Assertion Markup Language (SAML) V2.0 Technical Overview Work Draft 10*, 9 October, 2006, http://www.oasis-open.org/committees/documents.php?wg_abbrev=security, pp.5~27

Nie Li is a full time postgraduate student, College of Computer Science, South-Central University for Nationalities, PR China. She will graduate in June, 2008. Her research interests are in network security and applications.

Jiguang Lu is a Full Professor, College of Computer Science, South-Central University for Nationalities, PR China. He graduated from Wuhan University in 1968 as a postgraduate. His research interests are in network security and applications.

Research of Credential Chain Based on Attribute Authority

Jianyuan Gao
School of Computer Science and Technology, Hubei University of Economics
Wuhan, Hubei 430205, China
Email: gjygjy2000@163.com

ABSTRACT

On account of the current problem of application localization in micro-environment which is based on Privilege Management Infrastructure. This paper provides an authorization model named AAT which adapt to distributed application environment, and explains how to establish credential chain with maintenance at the same time, and then illustrates the credential issuing mechanism based on the credential chain. In the end, the paper gives a simulation for the model and the result shows its better practicability.

Keywords: Attribute Authority, Application, Credential Chain, Attribute Certificate

1. INTRODUCTION

At present, PMI (Privilege Management Infrastructure) has been put to use in E-government successfully, but there is more obstacle when it is carried into execution for common applications such as E-commerce. Although many company engineers throw themselves into the research of PKI/PMI and indeed they have implemented some applications, the ubiquitous problem is that most of the applications can only work in microenvironment but can not communicate each other securely.

The "YiZhengTong" technology scheme is pushed in China nowadays, but it is limited in expression of user's privilege information and hardly achieves safe communication among different applications[1], so the role of attribute authority in PMI can't be fully acted by CA. This paper just about aim at the safe communication among different applications which have been successfully applied in microenvironment and provides an authorization model named AAT based on the privilege management infrastructure. It presents the method of establishing and maintenance of the credential chain, and provides a useful scenario for distributed applications such as E-commerce.

2. AA AND APPLICATION

AA（Attribute Authority）is the pivotal role in PMI, and it affords applications' security via issuing and managing AC(attribute certificate), so it is trustee for applications' security problem. Strictly speaking, AA must completely comprehend the demands of security and access controlling of the applications which it answers for, and sometimes the securer of AA comes from inner application environment[2].

As a rule, one AA takes charge of one or several applications simultaneously, and one application's security is controlled by one or a few AAs, the relation shows in Fig.1. If an AA works for a few applications, it is essential that there is few sensitive content among the applications, otherwise there maybe engender a strict security problem because of AA securer's oversight. A number of applications may need several AAs work for it, because such application is duty-apart and often need some attribute certificates which are interrelated. For example, one application need two different AAs issuing ACs(attribute certificates) for it, but it can't be played by only one AA because of the AA securer's morality. Generally, one application only needs one AA acted as its security trustee.

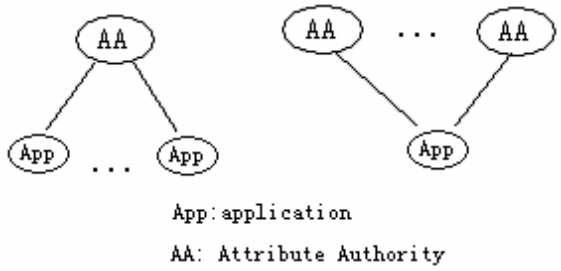


Fig.1. Relation between AA and application

There is a great demand of communication among different applications, such as the following case of E-commerce: a user in a company who has legal bank accounts (expressed with AC) can receive a discount when he makes a purchase order at an online shop which possesses a business license (expressed with AC), namely it is inevitable that the bank's application and shop's application will communicate each other. However, the shop doesn't always know the user's authenticity before the order is made, and the user doesn't know the shop's reliability, so it is essential for them to make a trust chain. The following passage will illustrate a trust chain model named AAT and describe how to establish accreditation.

3. CREDENTIAL CHAIN MODEL OF AA

3.1 Signification of Credential Chain

The types and amount of applications grow rapidly along with time goes on, when a new application is produced, sometimes the security is considered firstly. To avoid implementing the security module repeatedly for such application, we can adopt PKI/PMI scheme which is the security standard on Internet. As we known, a new application's security problem can be relegated to a believable third part AA, but if the AA securer does not know all details of the application or even can not know it as soon as quickly, how does the application realize its security?

As a matter of fact, in any application environment, there must be a organization such as some supervisors or securers which understand every security demand and know how to divide company staff into several different roles each of which should have a certain privilege, so it can act as the role of AA. Such AA only works in a microenvironment just for the application before it establish another trust relationship. For example, application 1 environment has its own AA(assume AA1) working for it, and another application 2 environment has its own AA(assume AA2) too; one day, there is a requirement that application 2 invite a certain role user from application 1 environment to have a discussion in application 2 environment.

Obviously application 2 doesn't assure whether a user from application 1 environment is just the proper user or not. At the time, they can solve this problem via an AC which can prove the user's role in application 1 environment, certainly it is just AA1 can do it. But how does AA1 know why or when to create an AC for the user? Perhaps there is only one probability that application 2 let AA1 know its desire. As a rule, AA1 does not know or even not believe application 2 but AA2, so only AA2 can do such job, it will tell AA1 what to do someway. We define such process as trust chain or credential chain, with example in Fig.2.

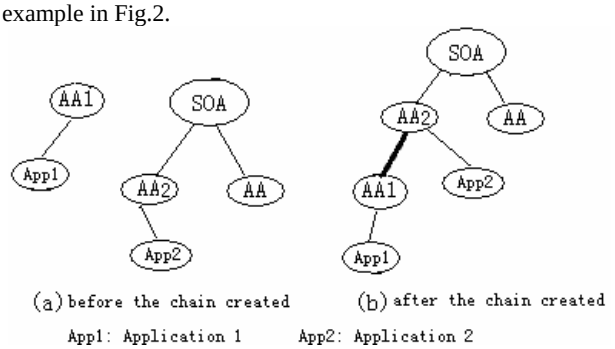


Fig.2. Credential chain

The bold line between AA1 and AA2 denotes the trust chain, it is mainly made up of four factors as follow:

formula 1: Trust_Chain =(source，target，value，session)

The source denotes the subject of trust chain, target denotes the object, value indicates the accreditation degree, and session includes some negotiating channels. With an idealized consideration, if AA2 believe AA1 completely, AA1 will fully believe AA2. The current theory and application about PMI are based upon it. However, the trust about two unfamiliar domains often doesn't reach a hundred percent. This is the primary reason of PMI applications localized in a microenvironment.

3.2 Means to Establish Credential Chain

This paper provides an integrated method of "bottom-to-top" and "top-to-bottom", for security of distributed environment applications, so as to form a larger believable domain.

The means of "top-to-bottom" similar to administration management, firstly an attribute authority named SOA will come into being, and later other AA who completely believe SOA will come from it, and even there can be more AA produced by its mother AA. These AAs build a trust-relationship tree shown in Fig.3, every AA take charge of one or two applications' access control. SOA is the root, and its son AA can be treated as its especial application, other AA works alike. Generally speaking, a son AA's privilege will be less than its mother AA and the son will believe its mother wholly, at the same time, the mother believe her son at the same accreditation degree. For example, a company is made up of a few subsidiary company, their parted applications maybe need to conform like real life.

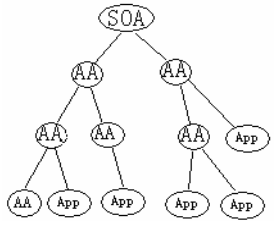


Fig.3. "Top-to-bottom"

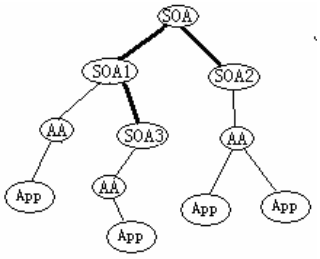


Fig.4. "Bottom-to-top"

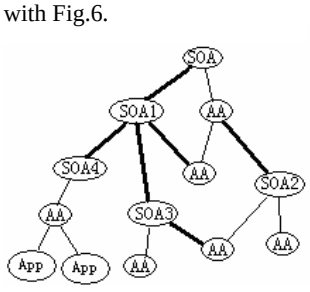
The means of "top-to-bottom" suit to principal and subordinate logic relation environment, but not adapt to equal logic relation environment. So another method "bottom-to-top" will work for the latter. When two unfamiliar applications want to have a secure communication through their own third party AA, it is essential that the two third party AA create their own credential chain like the section 3.1. We call it "bottom-to-top" with an example of Fig.4.

There are three basic already existed applications environment whose SOA are SOA1, SOA2, SOA3 respectively. All of the thin line show the complete accreditation which is usually created beforehand through the means of "top-to-bottom", and all of the bold line denote the credential chains which are created through the means of "bottom-to-top". As a rule, the former usually adapt to complete trust environment and the latter usually adapt to not complete trust environment. The latter case can happen randomly in the whole environment. So the AA credential chain topology will be very complicated. But if there are some controlling measures when a trust chain is established, the trust chain topology can be kept as a tree such as e-government, such topology is similar to CA topology. However numerous applications is more complex than e-government, when many new applications appear, the topology will vary rapidly.

3.3 Attribute Authority Topology

Because of the complexity of practical applications, we can hardly find the efficient measure to keep AA credential as a tree so as to hold a simple hiberarchy, what's more, even though we can do it, there will be more and more limits in applications. So we should not control the number of AA's credential chain or the level that AA belongs to, and so on. We should let it wholly meet the real life demand. And then AA topology can evolve from a tree to a net, for instance as shown in Fig.5. Apparently, SOA1, SOA2, SOA3, SOA4 denote four already existed applications environment, they can work normally at their own environment, each of them may be established through means of "top-to-bottom" or "bottom-to-top".

On the other hand, the credential chain shown in the front is too idealized. Actually, the value of credential chain can't reach a hundred percent and the chain often shows dissymmetrical. That is to say, A completely believe B, but perhaps B not completely or even completely not believe A, Furthermore, as time goes on, the degree of A believing B maybe descend. This is more frequent in distributed environment. So this paper use thick broken line with arrowhead to express such incomplete and dissymmetrical trust chain, and call such credential chain topology AAT(Attribute Authority Topology), for example with Fig.6.



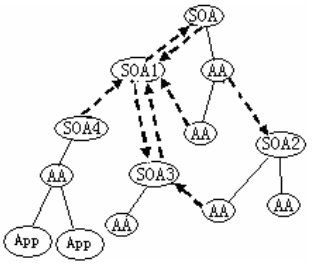


Fig.5. Tree-net shape topology **Fig.6.** Attribute Authority Topology

A thin line expresses the complete accreditation with each other, it is idealized and explicit in a microenvironment, once created, it will keep itself for long. So it is easy to establish and

maintain. A thick broken line with arrowhead express the unilateral and incomplete trust chain, but such trust chain usually change to another one in a little while. So we can find out In Fig.6 that, SOA4 directly believes SOA1 to some extent but SOA1 completely doesn't believe SOA4, SOA3 and SOA1 directly believe each other while the degree not always is the same.

In order to describe the dissymmetrical trust chain, a vector for the value of trust chain is introduced into this paper. It can easily indicate the variable AA topology. Assumed that AAi's trust value vector is Ci, it is expressed as formula 2.

Formula2: Ci=（Ci1,Ci2,...,Cij,…,Cin） $0 \leqslant Cij \leqslant 1, 1 \leqslant j \leqslant n$

Cij denotes the value of AAi believing AAj, apparently, Cii=1. If Cij=1, it says that AAi completely believe AAj; and if Cij=0, that denotes AAi completely doesn't believe AAj, otherwise if 0<Cij<1, it shows AAi doesn't completely believe AAj and the value is larger, AAj will be more worthy of confidence.

The algorithm of this trust chain value is pivotal in AAT. Along with the development of technology, an intelligent study module can be designed to calculate and update the vector. On the other hand, we can consider two factors including the current AA topology and the AA securer. The trust chain value can be calculated as formula 3.

Definition 1: Si={k | AAi directly believe AAk, that is, there is an edge <AAi,AAk>}.

formula 3: $Cij = E(i,j) \times Wi + (1-Wi) \times \frac{1}{|Si|} \sum_{k \in Si} (Cik \times Ckj)$

In formula 3, E(i,j) denotes the evaluated value of subject AAi for object AAj, it can be fixed by the securer through some means. Wi denotes the coefficient of such factor, |Si| denotes the element number of set Si, Cik×Ckj denotes the product of two trust chain value, and AAi directly believe AAk. E(i,j) and Cik×Ckj are variable, so Cij is variable. The communication among different applications will base on their AA's trust chain, if the value is too little, the communication will fail. That is to say, this model correlates communication with their credit standing. For example, if a website of E-commerce lose credit to users, it will become isolated from other AA for that, soon all users in the whole secure domain will not believe the website once more.

In a general way, if AAi has never communicated with AAj, the trust chain is null or keeps initial state with Cij=0. When two unfamiliar domains want to communicate, they will establish trust chain in virtue of the existed AA topology. When they have finished communication, they can keep their trust chain or let it descend along with time goes on. Any adjustment on trust chain maybe influence other trust chains, especially for the prestigious AA. The adjustment by a prestigious AA can bring snowball-rolling effect. So the interval of two times adjustment could neither be too short nor be too long. If too short, the cost of system resources can't be neglected; and if too long, there will be a hidden security trouble, that is, many innocent users may be cheated by a certain application which loses its credit for a long time. The author make an eclectic conclusion with eight seconds in simulation, and the result indicates that, when one AA loses its credit, eighty percent of all AA entities descend the value for it in two seconds, and others will react between two seconds and six seconds.

The establishment and dynamic updating can change the AA topology at any moment. If two domains break the trust chain drastically, they come back to their initial state. And if most domains break the trust chain drastically, they come back to the whole environment initial state. In addition, one AA may be revoked or removed from the application environment, it can also change the AA topology. All of these will lead to a new conformity, since it is complicated, it must evolve into a new topology that is more practical and close to real life.

3.4 Issue and Use of AC Based on AAT

Here we can use the example of section 3.1, supposing that the credential chain is established beforehand shown in Fig.7. That is to say, the certain role user from application 1 must get an AC that can prove his especial role and then the accessing to application 2 can be successful. There are two issuing AC manners as follows:

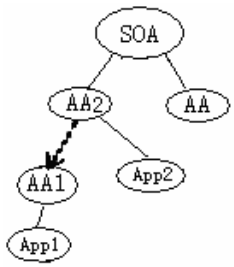


Fig.7. AC issue manners

(1) commission issue, This is an indirect manner that AA2 trusts AA1 with issuing the certificate. As a result of AA1 completely knows every one in the application 1 environment but AA2 not, and AA2 establish a credential chain with AA1, it can create an AC for AA1 and then AA1 may use it to create another AC for the application 1 users. So here AA1 is an especial application for the AA1. When the user put forward the AC to application 2, the certificate can be verified. When it was accepted the discussion will be done.

(2) direct issue, this is an direct manner for AA2 to issue AC, firstly the role user should get an AC which can prove his role from AA1(this step perhaps has been done before), and then the user put forward the certificate to AA2 and apply a new AC for the discussion. Since AA2 believe AA1 to some extent, so it can accept the certificate and create a new AC for the user to let him join their discussion even AA2 know little about the user.

The two manners also accord with two AA when their trust chain is indirect (there are some other AA connecting them), the difference is just the length of credential chain in AC. The first manner can avoid system bottleneck on AA2 because of the AC issue, however it will increase the time of AC verifying because of the credential chain. The second manner can make the AC verifying and managing more simple, but the creation of AC is more complicated than the former and easily result in bottleneck.

4. SIMULATION

In the interest of security and usability of AAT model, a test and simulation was designed as follows: create 100 random AA, and initialize some credential chain whose value stored in an array C[100][100], the default is 0, and set C[i][j] calculated again every other eight seconds in the program, in addition, let Wi=0 in the formula 3 to calculate C[i][j], it means that take no account of securer factor for the moment, every other second it

select two different AA via random function that mean to communicate with each other.

As a result of the simulation, as time goes on, more trust chain appears. About 2 minutes later, the trust chain goes into a wide range of trust chain closure[3]. Because the element of array C[100][100] never change for long. Within the experiment, if we add some other trust chain, we can find out about 40 seconds later, the topology reach another closure state. On the other hand, when the program call a function which randomly select a trust chain AAi, AAj, and then let C[i][j] equal 0. We can find out about two seconds later eighty percent of AA descend the trust value C[k][j] ($1 \leqslant k \leqslant 100$) and others react in six seconds. For real applications, blacklist technology can be added, it can make an application which lose credit standing and its third party completely insulated.

Additionally, the author of this paper make another test to simulate the process of AC issue, and the result mostly accord with expectation.

5. CONCLUSIONS

In this paper, we expatiated the AAT trust model which adapt to distributed environment, especially for the E-commerce applications and make a simulation for the trust model through a program, the result shows its better practicability and flexibility.

REFERENCES

[1] ISO/IEC9594-8, *Information telenology, Open Systems Interconnection The Directory, public-key and attribute certificate framework, Fourth edition[S*].2001.

[2] Gui Chao, Gao Jianyuan, Ge Ping, "Research of the Topology Problem of Core Infrastructure in PMI," *CONTROL & AUTOMATION*, 2006 Vol.22 No.3 pp. 62-64

[3] Xie Dongqing, Qin Dali, Liu Chunlei, "TREM-A Evaluated Model for Trust Relationship Based on Generalized Transitive Closure," *JOURNAL OF HUNAN UNIVERSITY(NATURAL SCIENCES)*, 2005 Vol.32 No.2 pp.113-117

Jianyuan Gao is an instructor from the School of Computer Science and Technology, Hubei University of Economics. He graduated from Huazhong University of Science & Technology and received his Master degree in 2005. His research interests are in E-Commerce, Network Security and complicated computation.

The Application of the AES in the Bootloader of AVR Microcontroller *

Jiaping Hong
Department of computer science, Hubei Normal University
Huangshi, Hubei 435002, China
Email: hongjiaping510@126.com

ABSTRACT

It is becoming more and more important how to protect the research result of the developer from being made copy the applied universality of the embedded system. Considering the application of the AES (Advanced Encryption Standard) in the AVR embedded system，the function, characteristic and the basic working principium of the AES are introduced, and the particular procedure of the application of the AES encryption arithmetic in the Bootloader of the AVR embedded system is discussed in detail.

Keywords: Bootloader, AVR Microcontroller, Advanced Encryption Standard, Encryption

1. INTRODUCTION

The efficiency and security of encryption have the relation with the length of grouping. The DES (Data Encryption Standard) encrypt the grouping data of 64 bits with the cipher of 56 bits, and the 3DES encrypt a plaintext to cryptograph by repeating arithmetic of DES three times with two or three times of the cipher. But the main shortcoming of the DES or 3DES is that the realization speed is slow at first, and that the security cannot be guaranteed secondly. The AES is the encryption standard by using the safety code, its length of grouping is 128 bits, and it can provide the enough safety.

2. REVIEW OF THE CRYPTOGRAPHY

2.1 Review of the AVR Microcontroller Encryption

Many AVR microcontrollers are configured such that it is possible to implement a bootloader able to receive firmware updates and to reprogram the flash memory on demand. The program memory space is divided into two sections: the Bootloader Section (BLS) and the application section. Both sections have dedicated lock bits for reading and writing protection so that the bootloader code can be secured in the BLS while still being able to update the code in the application area. Hence, the update algorithm in the BLS can easily be secured against outside access. This typically is not secure before it has been programmed into flash memory and lock bits have been set. This means that if the firmware needs to be updated in the field, it will be open for unauthorized access from the moment it leaves the programming bench or manufacturer's premises. The method that uses the AES to encrypt the firmware is to encrypt the data before it leaves the programming bench and decrypt it only after it has been downloaded to the target AVR. This procedure does not prevent unauthorized copying of the firmware, but the encrypted information is virtually useless without the proper decryption keys. Decryption keys are only stored in one location outside the programming environment: inside the AVR. The keys cannot be regenerated from the encrypted data. The only way to gain access to the data is by using the proper keys.

Such as in Fig. 1, the programmer or data is encrypted to be an outside plaintext; the microcontroller is first equipped with bootloader, decryption keys and application firmware. The bootloader receives the actual application and programs it into flash memory, while the keys are required for decrypting the incoming data. Lock bits are set to secure the firmware inside the AVR. A new release of the firmware is completed and there is a need to update products, which already have been distributed. The firmware is therefore encrypted and shipped to the distributor. The encrypted firmware is useless without decryption keys and therefore even local copies of the software do not pose a security hazard. The distributor upgrades all units in stock and those returned by customers. The encrypted firmware is downloaded to the AVR and decrypted once inside the microcontroller. Lock bit settings continue to keep the updated firmware secured inside the AVR [1].

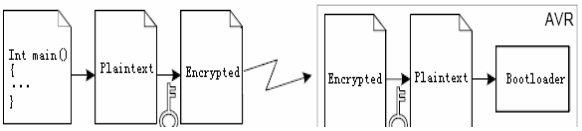


Fig.1. Overview of the AVR eneryption

2.2 Encryption

Encryption is the method of encoding a message or data so that its contents are hidden from outsiders. The plaintext message or data in its original form may contain information the author or distributor wants to keep secret, such as the firmware for a microcontroller.

2.3 Decryption

Decryption is the method of retrieving the original message or data and typically cannot be performed without knowing the proper key. Keys can be stored in the bootloader of a microcontroller so that the device can receive encrypted data, decrypt it and reprogram selected parts of the flash or EEPROM memory. Decryption keys cannot be retrieved from the encrypted data and cannot be read from AVR microcontrollers if lock bits have been programmed accordingly.

3. AES ENCRYPTION

The flowchart of the AES encryption process is shown in Fig.2. In the encryption process, most block ciphers consist of a few operations that are executed in a loop a number of times. Each loop iteration uses a different encryption key. At least one of the operations in each iteration depends on the key. The loop iterations are referred to as encryption rounds, and the series of keys used for the rounds is called the key schedule. The number of rounds depends on the key size. Each step is implemented as a subroutine for convenience. Using an optimizing compiler remove the unnecessary function calls to save code memory

* This paper is supported by the Natural Science Foundation of Hubei Province of China under Grant No.2004ABA023.

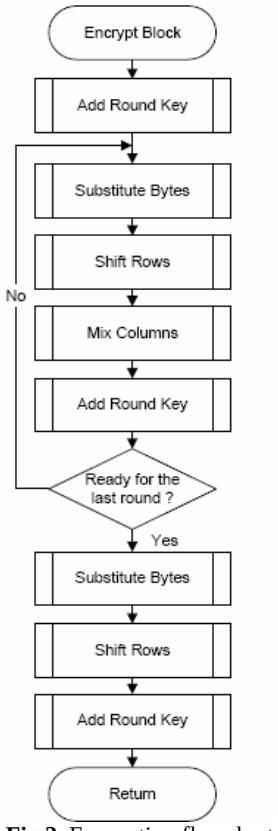


Fig.2. Encryption flowchart

4. THE APPLICATION METHOD OF AES IN THE BOOTLOADER OF AVR MICROCONTROLLER

The bootloader must reside in the target AVR before the device can be updated with encrypted firmware. The bootloader communicates with the PC and is capable of programming the EEPROM and the application area of the flash memory.

This and the following subsections describe how to use and configure. the applications. The process is illustrated in Fig. 3, the main steps are as follow:

(1) Create an application for the target AVR, if required, and create an EEPROM layout in a separate file;

(2) Create a configuration file with project dependent information. The application called gentemp can be used for creating a file frame;

(3) Run the application files. This will create the header file, key file and the encrypted file; using IAR EW (Embedded Workbench), configure. and build the bootloader for the target AVR;

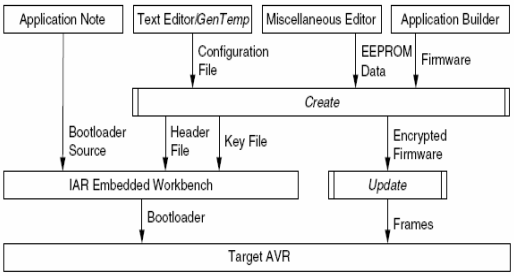


Fig.3. Overview of project flow

(4) Download bootloader to target AVR and set lock and fuse bits;

(5) The encrypted firmware may be downloaded to the AVR at any time. [2] The detailed steps are as follows.

At first, download the file of the "AVR_AES.zip" from http://www.ouravr.cn/bbs/bbs_upload1892/files_5/armok0193046.zip, after decompression，two folders (IAR and PC) are produced; The IAR folder contains the update firmware, and the PC folder contains the update programmer of PC. The following is the process:

(1) Run the file"..\ PC Sample\Gen_Key.bat" and the provisional file "config.txt" is produced. The format of command "Gen_Key.bat" is:
Gentemp Config.txt
The following is the example of the file "config.txt" produced:
PAGE_SIZE= [FILL IN: Target AVR page size in bytes]
MEM_SIZE= [FILL IN: Application Section size in bytes]
CRC_ENABLE= [FILL IN: YES/NO]
KEY1 =5F8669C385D366FAF49FEA4F23D983D34616
KEY2=F3F6340CEC9B0B4B0C
KEY3=972CEE3391BC6C5F93
ITIAL_VECTOR=39D392DFD0259A0EAE85C9D4A11 DF1CC
SIGNATURE=A87DB128
Run the "Gen_Key.bat" every time, and the interrelated parameters such as： KEY, INITIAL_VECTOR and SIGNATURE are obtained; but their results are not the same. But the same item must use the parameters of KEY, INITIAL_VECTOR and SIGNATURE by running the command"Gen_Key.bat"produced at one time.

(2) According to the chosen MCU， modify the file "config.txt", and set rightly the parameters such as PAGE_SIZE, MEM_SIZE and CRC_ENABLE. Regarding the ATMEGA32 as the example (such as in Fig.4), its interrelated parameter can be installed as follows:
PAGE_SIZE=128
MEM_SIZE=28672

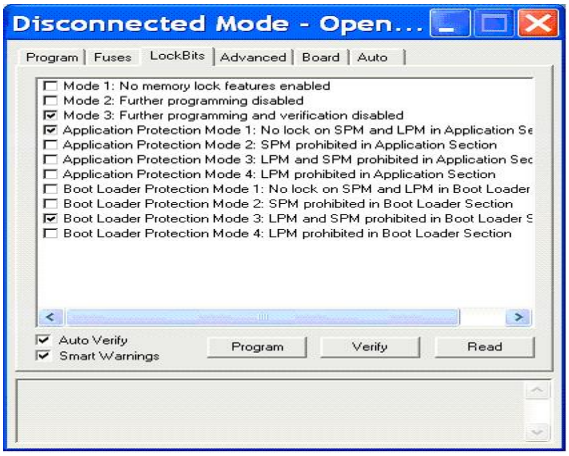


Fig.4. the windows of setting parameters

CRC_ENABLE=YES
KEY1=5F8669C385D366FAF49FEA4F23D983D346 16KEY2=F3F6340CEC9B0B4B0C
KEY3=972CEE3391BC6C5F93
NITIAL_VECTOR=39D392DFD0259A0EAE85C9D4A 11F1CC
SIGNATURE=A87DB128

(3) Run the file"..\ PC Sample \Create_Header.bat", and the provisional file "BootLdr.h"and "AESKeys.inc" is produced. The format of command "Create_Header.bat" is:
Create -c config.txt -h bootLdr.h -k AESKeys.inc

(4) Copying the file"BootLdr.h" and"AESKeys.inc" to the folder…\AVR_AES\IAR, and compile them again. Be sure to set rightly the UBRRL according to the actual circumstance, such as the setting of the communication parameter following：[3]

```
Void busInit (void)
 {
 // 115200 baud @ 3.6864MHz
 UBRRL=1;
 // 9600 baud @ 3.6864MHz
 // UBRRL=23;
 // Enable Rx and Tx.
 UCSRB= (1 << RXEN) | (1 << TXEN);
 }
```

(5) Such as in Fig. 5,Read-in the bootloader of the Atmega32 MCU with the hex file, and set right the Lock Bits.

(6) Run the file "..\PC Sample\ Encoding Firmware. Bat", the encrypted the source file will be updated, and then the encryption file "NewFlash.ext" which will be produced. The format of command "Encoding Firmware.bat" is:
Create -c Config.txt -f main. hex -o NewFlash.ext -l BLB11 BLB12

The encryption file "NewFlash.ext" in the file "main. hex" is produced according to the file "Config.txt", and set right the lock bits "BLB11 BLB12". If the file "eeprom.hex" is encrypted, it will be realized by modifying the file "Encoding Firmware.bat", and then the encryption file "NewFlash.ext" is produced. The format of command "Encoding Firmware.bat" is：

Create -c Config.txt –e EEPROM.HEX -f main. hex -o NewFlash.ext -l BLB11 BLB12

(7) Turning on power, and run the file"..\PC Sample\ Updated.bat". The format of command "Updated. bat" is：Update NewFlash.ext -COM1 -115200

The command mentioned above means that it would send the encryption file "NewFlash.ext" from the COM1of the PC to MCU，and set the baud rate as 115200.
Download the program to the chosen MCU finally, and then restart and run it.

5. SOME POINTS OF NOTICE IN THE AES BOOTLOADER

Before running the bootloader, the bootloader must be compiled and then downloaded to the target AVR Studio being used. The following fuse bits must be configured:

(1) Size of the bootloader section. Set fuse bits so that the section size matches to the BOOT_SIZE setting.

(2) Boot reset vector. The boot reset vector must be enabled.

(3) Oscillator options. The oscillator fuse bits are device dependent. They may require configuration.

(4) The bootloader supports downloading in an encrypted form. When the bootloader is first installed it must be equipped with decryption keys, required for future firmware updates. The firmware can then be distributed in an encrypted form, securing the contents from outsiders.

(5) It is recommended to program lock bits to protect both application memory and the bootloader, but only after fuse bits have been set. Lock bits which can be programmed using AVR Studio.BLS lock bits will also be set during firmware updates, provided that they have been defined as command line arguments when the firmware is encrypted [4]- [7].

Fig.5. setting of the read-in Bootloader of the embedded system with the hex file

6. CONCLUSIONS

This paper has presented a method for transferring data securely to an AVR microcontroller with bootloader capabilities by using the AES, and has also highlighted techniques that should be implemented when building a secured system. The bootloader may also be used to erase the application section, if required. Many attack attempts include removing the device from its normal working environment and powering it up in a hacking bench.
In applications where it is not feasible or possible to use an external communications channel for updates, the firmware can be stored in one of Atmel's Crypto Memory devices. The memory can be packaged as a removable smart card, which can easily be inserted in a slot of the device when an upgrade is needed. The microcontroller can check for the presence of a Crypto Memory upon startup and retrieve a firmware upgrade as needed.

REFERENCES

[1] Verbauwhede I M.Schaumont P R.Kuo H. "Deign and performance testing of A 2.29 Gb / s rijndael processor," *IEEE J.of Solid State Circuit, March J.of Solid State Circuit*, March 2003, 38(3): 569—572

[2] Henry Kuo.Ingrid Verbauwhedc. "Architectural optimization fora 1.82Gbits / sec VLSI implementation of the AES Rijndael algorithm," *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, 2001,51—64.

[3] Anna Labb6.Annie P6rez and Jean Michel Porta1."Efficient hardware implementation of crypto -memory based on AES algorlthm and SRAM architecture," *IEEE International Symposium on Circuits and Systems* May.2004.

[4] James Nechvatal, Elaine Barker, Lawrence Bass ham *et a1*. "Report on the development of the Advanced Encryption Standard (AES)," *National Institute of Standards and Technology*，2000 (10): 623—656.
[5] Atmel Corporation: AES Bootloader. 2005.4.
[6] Ming ZHANG, Hou-jing CHENG and Fang SUN: "The Application Method of the Bootloader Software of the ATMega48" in *Microcontroller and Embedded System in Chinese*. 2005（8）
[7] Richard Barnett, Larry O'Cull, and Sarah Cox: *The Program of Embedded C and AtmelAVR* in Tsinghua University Press in Chinese. 2003.9.

Jiaping Hong, male, Chinese, was born in December 1964, Sub-professor, a teacher of the department of computer science of Hubei normal university. He's research focus is the application of the embedded system.

Using AOP Concepts to Improve Web Security Patterns

Peichao Guan
School of Computer Science and Technology, Hubei University of Economics
Wuhan, Hubei 430205, China
Email: gpc@hbue.edu.cn

ABSTRACT

AOP (Aspect-Oriented Programming) offers us a new perspective analysis and systems design, with which problems involved in crosscutting concerns and software design can be approached well. In process of developing a practical website, system designers and programmers usually strive for some similar security needs which can be met by employing available and mature security patterns or by using AOP concepts to redesign programming patterns. The purpose of the paper is to discuss a strong method for web security architecture and then provide a method to design and implement the web security pattern by using AOP paradigm.

Keywords: Aspect-Oriented Programming, Aspect-Oriented Design, Security Patterns, Secure Logger Pattern, Web Service

1. INTRODUTION

Web-based software development has become prevalent nowadays. Web security, as guarantee in web service, is carried out by an array of characters, each of which serves as defense or solution of potential risks and flaws in systems. In different kinds of web service development life cycles, security, as one of nonfunctional requirements, is applied to different levels of software systems, normally in the last period of the software development. Experience demonstrates this is not proper. We should adopt and implement end-to-end security in the beginning of practical design and development; otherwise, once systems are confronted with security attack, available remedy which can work afterwards cannot repair flaws made in design period.

Among the existing solutions, many researchers have talked about security pattern[1, 2], employing a secure unified procedure to regulate the process of software development, including security requirements, security architecture, security implementation, White-box Testing, black-box Testing, monitoring, security auditing, and so on. It is obvious that these activities are related to different periods in software development life cycle, with security architecture as core in the process. Software designers should follow compulsory security requirements demanded by system analyst and create security architecture draft as backup, which decides a series of security patterns to implement known security requirements and attack potential flaws in systems. Many web security pattern focused on approaching and applying common information security involved in basic security equipments can be found in existing data resources. The common in these security patterns, most of which stem from design patterns presented by the Gang of Four, is the idea based on object-oriented design.

Conventional object-oriented software development can attack single programming problem in business logic layer, but with intrinsic limitation when it comes to crosscutting concerns and problem that how to respond to variable requirements. The same limitation exists in conventional security patterns based on OO techniques. Aspect-oriented programming (AOP) [3, 4] is one of paradigms created by Xerox Palo Alto Research Center in 1990s. It enables programmer to separate tasks (crosscutting concerns) that should not be tangled better and then provide program with better encapsulation and interoperability. The central idea of AOP is to consider complex system as a combination of several concerns. Under the help of AOP tools, software designers can improve the existing web security patterns.

2. THE CONCEPTS OF AOP

AOP, the same as OOP, is not a programming language itself, but a kind of software design idea, a paradigm. Look back to the history of software design, program design has developed from machine-oriented programming to process-oriented programming, to object-oriented programming, and to component-oriented programming. Each of these software methodologies provides increasingly natural method to convert system requirements into program designs. With the advancement of the software methodologies, it becomes easier for program designers to understand and create more complex systems. However, AOP is not born to replace OOP. It is a sort of complement or improvement for OOP which changes perspective and paradigm of software development solves problems overlooked by OOP and unsettled issues, and enables programmers to land separation of tangled responsibilities, such as core business logic and authentication handling.

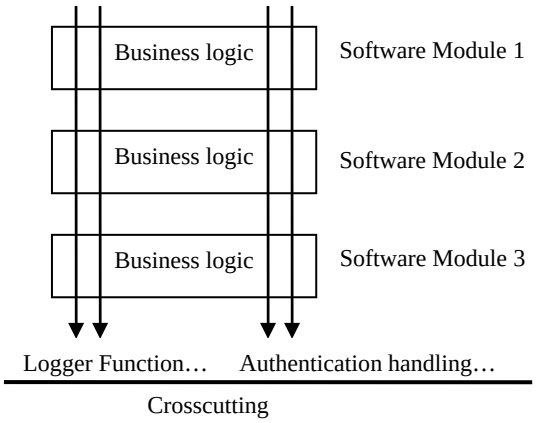


Fig.1. Crosscutting Concerns and Business Logic

To comprehend the essential idea of AOP, we should have a better understanding of concerns. Simply put, a concern is a specific goal or an area of interest [5]. Concerns fall into two categories: core concerns and system concerns. The former includes business logic while the latter includes logging, authentication, security, performance, persistence and so forth. Because system concerns are related to implementation of separate modules, system concerns are called crosscutting concerns.

Fig.1 show that, by employing its implementation, AOP allows us to program crosscutting concerns directly [6], which cannot be reached by employing OOP. Obliviousness and quantification are two major characters in AOP. The former indicates that programmers cannot make it clear whether aspect code will be executed by checking basic code in programs. That is the main advantage of AOP, which allows programmers to separate concerns as much as possible in the process of system design. Systems created under the idea of AOP can demonstrate quantification (such as Composition Filters [7] and synchronous advice [8]) by the way components are encapsulated by employing aspects. AOP implementation with lower-level granularity, such as programming language AspectJ[10] designed for common goals, allows for quantification in component inner mechanism. Quantification, to great extent, can help programmer avoid redundancy in process of design and code repetition.

Security can be viewed as a crosscutting concern in web application security [11] and the conventional nonfunctional application can be achieved under the help of Aspect-Oriented Software Development (AOSD). Also, it can be achieved by improving the existing security patterns with AOP concepts.

3. THE EXISTING WEB SECURITY PATTERN

According to Trusted Computer System Evaluation Criteria, all trusted applications need secure logging function. Logging, which can be used to debug and used as evidence in many web application environments, must be guaranteed as security in order for it to be protected from being purloining or operation by attackers. All events happening in period of web system operation should be logged selectively and correctly. Without log files, administrators will not be able to obtain evidence of attackers' activities or make sure consistency and validity of system data. The limitations of using logging function are the need of logging sensitive information which is not accessible for unauthorized users, the need of keeping consistency of log files, the need of unified system administration and necessary data encryption policy for confidentiality.

3.1 A conventional web-based Secure Logger Pattern

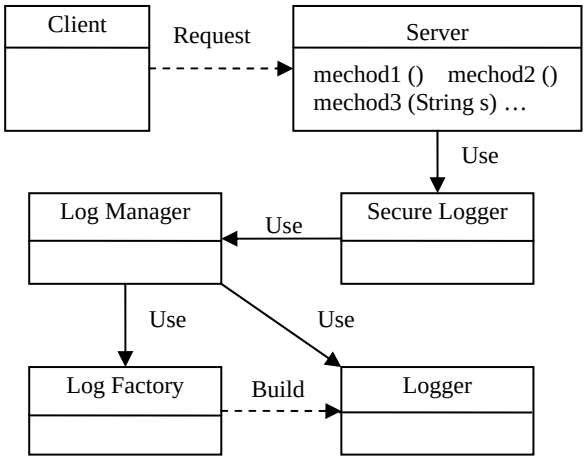


Fig.2. Normal Secure Logger Pattern

Fig.2 presents a normal secure logger pattern, in which request send by the Client to the server. The server responds relevantly after making authorization decision and logging Client operations selectively. Secure Logger class guarantees the data security, while Log Manger class takes the responsibility of writing data into log.

3.2 Limitation of the existing patterns

While conventional Server is making security log, code is spread selectively across several modules and specific components. That server depends heavily on Secure Logger brings about following limitations of web system created under such pattern [11, 12].

1) Codes for implementation of system businesses (here is log) are redundant among several components. That means, once programmers want to modify these businesses, they have to go to each of relevant modules.
2) Some components in Server are strongly coupled with Secure Logger, which increases difficulty in test [13].
3) Components in Server will become tangled because of codes unrelated to core businesses. For example, function of deleting log should only focus on how to find the right place of the log and then delete it, but rather focus on how to log the Client calling this function.
4) It is difficult to modify, maintain, and update the Logger. For example, Logger has to be modified constantly due to the changing application.

4. IMPROVEMENT OF PATTERN

The limitations of conventional Web Secure Logger Pattern mentioned above can be eliminated by employing efficacious implementation of AOP and the two characters (obliviousness and quantification) of AOP Concepts.

4.1 Add aspect to pattern

In the period of web-based application design, system security functions unrelated to specific application can be separated, according to security requirements from Requirement Analysis. Fig.3 shows the improved security pattern.

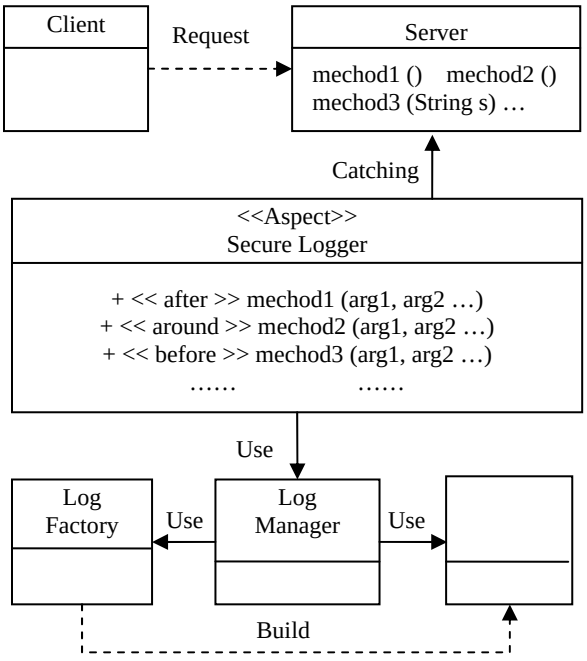


Fig.3. Improved Secure Logger Pattern

The limitations in web-based security pattern, to some extent, can be eliminated by employing new pattern [14]. Convert Secure Logger into an aspect component in the period of system design. The process of analysis and implementation of basic business logic can leave alone log aspect, which demonstrates better application modularity and obliviousness of AOP. Implementation of modularization of logging functions commonly concerned in several business logics in system brings about convenience in analysis, design, implementation, and maintenance. Also, it enhances robustness and flexibility which reflect multidimensionality of AOP.

4.2 Realization

Many tools of AOP can be used to construct the mentioned aspect-oriented web security pattern. The following two methods are commonly and effectively used to realize it.

1) Based on Spring: Spring AOP is part of the Spring Framework Open Source project [15], which purposes to simplify the development of J2EE applications. AOP modules in Spring, as basis of developing aspect-oriented programs for application system of Spring, provide full support to compatible AOP aspect-oriented programming. Programmers are allowed to define interceptor and pointcut for clear decoupling of function implementation codes which should be logically separated. Different operation information can be combined into codes by employing source-level metadata.

   Spring AOP is realized by pure Java, which does not need particular compilation (unlike to AspectJ providing special compilation environment, with lower level of granularity). Spring can support intercepting method calls, but member variable interceptor has not been realized yet. Although adding term interceptor lend support (rather than destroy) to the central API of Spring AOP (To someone, term interceptor is of potential danger, pointing out that encapsulation in OOP requires using method calls to access certain filed and encapsulation will be destroyed if the filed is accessed directly by employing AOP implementation), intercepting method calls are enough for common application.

   In Spring, the way to create AOP proxy is employing ProxyFactoryBean class provided by framework which enables programmers fully control the pointcut, enhanced issues that should be controlled, and the order of them. Declare necessary pointcut or issues needed enhancement, in the form of object. Then, declare an object that will be enhanced, and create a ProxyFactoryBean case which will replace the object and used by user.

```
import java.lang.reflect.Method;
import org.springframework.aop.MethodBeforeAdvice;

public class SecureLoggerAspect extends
   MethodBeforeAdvice {
   ……
   public void before(Method m, Object[] args, Object
target)throws Throwable {
         // obtain needed log class, write log
   }
   ……
}
```

Fig.4. Improved Secure Logger Class

   While employing AOP techniques of Spring for realization of secure log pattern, SecureLogger class should be rewritten into SecureLoggerAspect class, inheriting MethodBeforeAdvice interface from Spring framework, realizing “before” method. Thus method calls in Sever can be intercepted, as Fig. 4 shows.

   XML files take the responsibility to implant aspects (Secure Logger class) into Server methods calls indicated, so dependence of Server on Secure Logger class can be eliminated in the old pattern. Fig.5 shows a segment of relevant XML configuration file.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD
BEAN//EN"
"http://www.springframework.org/dtd/spring-beans.dtd">

<beans>
<bean id="SecureLogger" class=" SecureLoggerAspect "/>
<bean id="bean" class=
"org.springframework.aop.framework.ProxyFactoryBean">
        <property name="proxyInterfaces">
            <list>
        <value> here are classes in Sever </value>
        <value>……</value>
        <value>……</value>
            </list>
        </property>
        <property name="interceptorNames">
            <list>
                <value> SecureLogger </value>
            </list>
        </property>
  </bean>
……
</beans>
```

Fig.5. XML file for weaving

2) Based on AspectJ: The first versions of AspectJ were released in 1998 and, as of December 2002, the AspectJ project has left Palo Alto Research Center and joined the open-source Eclipse community [16]. Today, AspectJ is the most widely used aspect-oriented language which can weave methods calls, filed accesses, object construction, and exception. It is the implementation of AOP of lowest-level granularity, and makes the lowest loss of performance. Also, when it comes to a crosscutting problem, codes created under AspectJ are as effective as codes written by programmers but with much better modularity.

```
import java.util.logging.*;

public aspect SecureLoggerAspect{
  pointcut outputLog() : call(public void method*());
  before() : outputLog() {
   Logger theLogger = Logger. getAnonymousLogger();
  theLogger.info("Calling method ! ");
  }
  pointcut uniqueLog(String s) :
        call(public void mothed3(String))&&args(s);
  before(String s) : uniqueLog(s) {
   Logger theLogger = Logger. getAnonymousLogger();
  theLogger.info(s+" is Calling method3 ");
  }
……
```

}

Fig.6. Aspect Realization Based on AspectJ

Because AspectJ provides aspects of language-level and language that can define pointcuts [17], SecureLogger can be rewritten into SecureLoggerAspect in order to eliminate dependence of Server on SecrueLogger while programmers are employing AOP techniques provided by AspectJ to realize secure log pattern, as Fig. 6 shows.

4.3 Brief evaluation

The basic purpose is to separate system concerns and eliminate the dependence between specific business logic and security concerns, no matter which AOP tool is used to improve web secure patterns. For some common applications, no compiler is needed while using AOP in XML files, and it becomes more convenient for implantation. AspectJ can server as a backup if "crosscutting" of low-level granularity objects is needed in the process of improving pattern.

5. CONCLUSIONS

With the rapid advancement of web application, it becomes increasingly urgent to construct systems with good maintainability and modularity. Almost all the existing web security patterns are designed based on OOP which brings about complication of application, strong coupling in system, disappointing reusability and maintenance, and has a negative impact on fast software development and implantation.

We have described improvement of a common web secure pattern and the process of using it, which has demonstrated its advantage. Using AOP concepts and techniques properly and adopting the improved OOP patterns in the period of analysis and design of web application make development of web application system more effective and stronger. It is can be predicted that AOP-based ASOD will pervade through every period and layer of software development and become influential.

REFERENCES

[1] Rosado, D.G., Gutierrez, C., Fernandez-Medina, E., Piattini, M., "A study of security architectural patterns, Availability, Reliability and Security," 2006. *The First International Conference* on Vol. Iss., 20-22 April 2006, pp8.

[2] Laverdiere, M-A.; Mourad, A.; Hanna, A.; Debbabi, M., Security Design Patterns: "Survey and Evaluation, Electrical and Computer Engineering," *Canadian Conference* on, Vol. Iss., May 2006, pp1605-1608.

[3] Robert J. Walker, Elisa L. A. Baniassad and Gail C.Murphy, "An Initial Assessment of Aspect-oriented Programming," In *Proceedings of the 21st International Conference on Software Engineering*, May 1999.

[4] Kiczales, G., "Aspect-oriented programming, Software Engineering," 2005. ICSE '05. *Proceedings of the 27th International Conference* on, Vol., Iss., May 2005, pp730.

[5] Griswold, W.G.; Shonle, M.; Sullivan, K.; Song, Y.; Tewari, N.; Cai, Y.; Rajan, H., "Modular software design with crosscutting interfaces," *Software, IEEE,* Vol.23, Iss.1, Jan-Feb 2006, pp51-60.

[6] Zhen Hua; Zhen-Chong Wang; Jun Hua; Gong-Xun Yang; Yan-Wu Liu, "The Framework of Agent-Oriented Programming," "Machine Learning and Cybernetics," 2005. *Proceedings of 2005 International Conference* on, Vol.1, Iss., 18-21 Aug. 2005, pp282-286

[7] Bergmans, L. and Aksit, M. "Composing crosscutting concerns using composition filters." Comm. ACM 44, Oct 2001, pp51-57.

[8] Holmes D, Noble J and Potter J, "Towards reusable synchronization for object-oriented," In *workshop on Aspect-Oriented Programming* (ECOOP), 1998.

[9] Lesiecki, N, "Applying AspectJ to J2EE application development," *Software, IEEE,* Vol.23, Iss.1, Jan-Feb 2006, pp.24-32.

[10] John Viega, Bloch J T, Pravir Chandra, Appling Aspect Oriented Programming to Security, Cutter IT Journal, November 2002, pp.57-60.

[11] Laddad, R, "Aspect-oriented programming will improve quality," *Software, IEEE,* Vol.20, Iss.6, Nov.-Dec. 2003, pp90-91.

[12] Miller, S.K., "Aspect-oriented programming takes aim at software complexity," Computer, Vol.34, Iss.4, Apr 2001, pp18-21.

[13] Nadia Belblidia; Mourad Debbabi; Aiman Hanna; Zhenrong Yang , "AOP Extension for Security Testing of Programs, Electrical and Computer Engineering," *Canadian Conference* on, Vol., Iss., May 2006, pp647-650.

[14] Bernardi, M.L.; Di Lucca, G.A., "Improving Design Pattern Quality Using Aspect Orientation, Software Technology and Engineering Practice," 2005. 13th *IEEE International Workshop* on, Vol., Iss., 24-25 Sept 2005, pp206-218.

[15] SPRING Group, SPRING/AOP website, http://www.springframework.org, 2007.

[16] ASPECTJ website, http://eclipse.org/aspectj/, 2007

[17] Ramnivas Laddad, "AspectJ in Action: Practical Aspect-Oriented Programming," *Book News*, Inc., Portland, 2004

Peichao Guan, lecturer of School of Computer Science and Technology of HuBei University of Economics, received bachelor degree from Computer Science College of HuBei university in 1999 and master degree from International Software College of WuHan university in 2007. He has participated in publication of three books and written four academic papers. His research interests are in Software Engineering and Principle of Compiler.

Research on Automated Trust Negotiation in Grid Environment

Hongwei Chen
School of Computer Science and Technology, Hubei University of Technology
Wuhan, Hubei Province, 430068, China
Email: chw2001@sina.com

ABSTRACT

Grids support dynamically evolving collections of resources and users, usually spanning multiple administrative domains. However, how to establish trust among strange domains without prior relationship and common security domain posed much difficulty for these resource sharing. Automated trust negotiation (ATN) is an approach which establishes trust between strangers through the bilateral, iterative disclosure of digital credentials. In this paper, an ATN model in Grid Environment, policy sets, negotiation strategy and negotiation protocol are presented. The main process of ATN includes: establishment of policy sets, converting policy sets into disclosure graph which improves Method Yu, reducing disclosure graph to disclosure tree, converting disclosure tree into disclosure sequence, and establishment of negotiation protocol.

Keywords: Automated Negotiation Trust, Disclosure Tree, Disclosure Graph, Disclosure Sequence, Grid Computing, Autonomic Domain

1. INTRODUCTION

Grids support dynamically evolving collections of resources and users, usually spanning multiple administrative domains. The Grid Computing environment provides its users with seamless access to every resource that they are authorized to access, enabling transparent sharing of computational resources across organizational boundaries. As a Grid grows larger and as jobs become more complex, seamless authorization and authentication becomes harder to provide [1]. The proliferation of the Grid Computing has given opportunities on different entities to share resources or conduct business transactions. However, how to establish trust among strangers without prior relationship and common security domain posed much difficulty for these activities. Automated trust negotiation is an approach which establishes trust between strangers through the bilateral, iterative disclosure of digital credentials [2]. Since credentials may be sensitive, access control policies can be used to control the disclosure of the credentials themselves. There are a number of open research projects such as TrustBuilder[3] and PeerTrust[4] in this area.

2. NEGOTIATION MODEL

Fig.1 is an ATN (Automated Negotiation Trust) model based on peer-to-peer collaboration pattern in Grid environment. This model mainly includes three modules: Trust Credential and Policy Sets, Negotiation Strategy and Negotiation Protocol. The ATN Service module mainly manages the above three modules. Trust credential is a kind of digital assertion signed by certificate authority. Trust credential encompasses attribute information of owner. The purpose of trust credential is to protect sensitive information resources. Policy sets define trust sets required by protective resource, and they are the basis of ATN. Negotiation Strategy is a mutual collaborative process of the grid service demander and grid service provider, and it is a constructive process of trust credential disclosure sequence. Negotiation protocol defines how to interact and exchange trust credential between grid service demander and grid service provider.

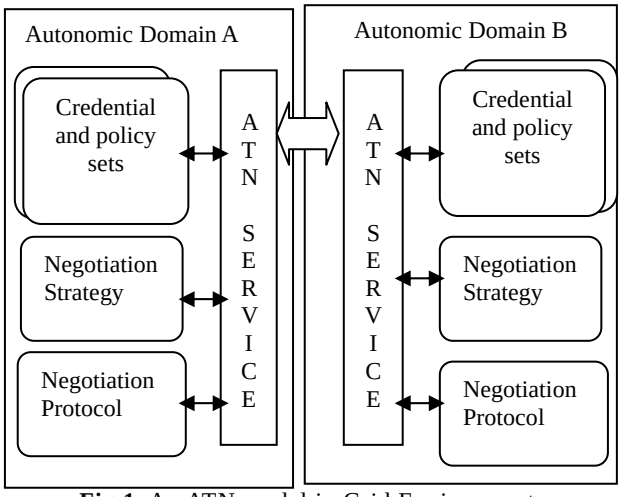


Fig.1. An ATN model in Grid Environment

3. TRUST CREDENTIAL AND POLICY SETS

Policy Sets includes the following basic expressions:

(1) $C \leftarrow A$: If one side wants to obtain trust credential C from the other side, it must provide trust credential A for the other side first.

(2) $C \leftarrow TRUE$: If one side wants to obtain trust credential C from the other side, it needn't any preconditions.

(3) $C \leftarrow A \wedge B$: If one side wants to obtain trust credential C from the other side, it must provide trust credential A and B for the other side first.

(4) $C \leftarrow A \vee B$: If one side wants to obtain trust credential C from the other side, it must provide trust credential A or B for the other side first.

In Fig.2, suppose that the following expressions are ATN Policy Sets from Autonomic Domain A and B. A is a grid service demander, while B is a grid service provider. If A want to obtain grid service, A must get hold of Trust Credential B0 from B.

A:	B:
$A1 \leftarrow B1 \wedge B2$	$B0 \leftarrow (A1 \wedge A2) \vee A5$
$A2 \leftarrow B3$	$B1 \leftarrow A2$
$A3 \leftarrow B1 \vee B2$	$B2 \leftarrow A4$
$A4 \leftarrow TRUE$	$B3 \leftarrow TRUE$

Fig.2 Example of Policy Sets

4. NEGOTIATION STRATEGY

Negotiation Strategy is a disclosure sequence constructed of trust credentials which are applied to mutual automated trust establishment of grid service demander and grid service provider. The following several steps are necessary for establishment of disclosure sequence: (1)To convert policy sets into disclosure graph.(2)To reduce disclosure graph into disclosure tree, which improves Method Yu [5].(3)To convert disclosure tree into disclosure sequence.

Fig. 3 illustrates how to convert negotiation strategy into disclosure graph. According to conversion method from Figure 3, rules of Policy Sets of Autonomic Domain A and B from Figure 1 will convert to disclosure graph from Figure 4. Because Autonomic Domain A doesn't encompass trust credential A5, we can insert a temporary and non-infective rule $A5 \leftarrow FALSE$ into the above example of Policy Sets.

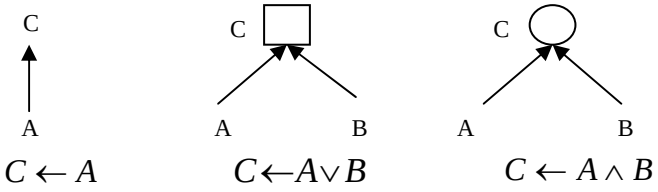


Fig.3. Conversion from Rules of Policy Setsto denotations of Disclosure Graph

However, there exist many redundant nodes and lines in disclosure graph. So we can reduce disclosure graph in term of the following redundant rules (Suppose that A represents grid service demander and B represents grid service provider).

(1) Rule 1: In the process of mutual negotiation interaction between A and B,B has a final objective credential which symbols the end of disclosure process. This trust credential is also named objective node. The out degree of the objective node is zero, which is means that the objective node doesn't point to any other nodes.
(2) Rule 2: If any nodes TRUE are existed in disclosure graph, then nodes TRUE and their linked lines can be erased.
(3) Rule 3: If any nodes FALSE are existed in disclosure graph, then all nodes and linked line along the path from node FALSE to the objective node can be got grid of except the objective node.
(4) Rule 4: If there existing any other nodes which out degree are zero except the objective node, then they can be erased, and their linked lines can be deleted.
(5) Rule 5: If existing a ring in disclosure graph, then erasing some lines to wipe off the ring.

After the above processing of redundant rules, disclosure graph can be reduced to a disclosure tree. In term of the above rules, disclosure graph from Fig.4 can be reduced to disclosure tree from Fig.5. The following contents are the redundant rules:

(1) According to Rule 1, B0 is the final objective node.
(2) According to Rule 2, it is necessary to wipe off TRUE nodes, and linked lines TRUE→A4 and TRUE→B3.
(3) There is no trust credential A5 in domain A. According to Rule 3, nodes FALSE and A5 can be erased, and the linked lines FALSE→A5 and A5→B0 can be deleted.
(4) Node A3 is a node which is out degree is zero. According to Rule 4, A3 could be deleted, and the linked line B1→A3 and B2→A3 can be deleted.
(5) Nodes A1, B1, A2 and (A1 ∧ A2) have formed a ring in Figure 4. According to Rule 5, the linked line A2→B1 can be got rid of.

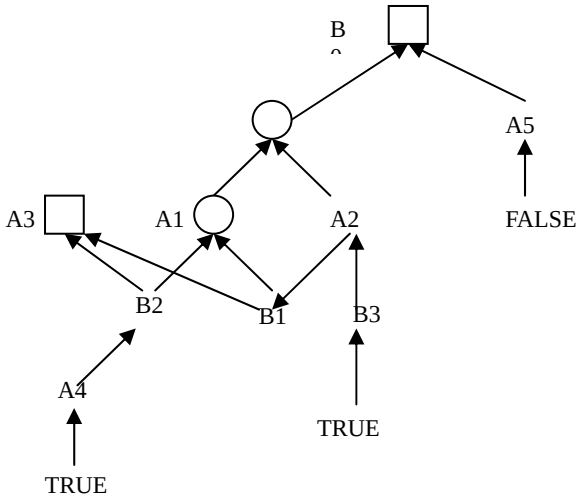


Fig.4. Example of Disclosure Graph

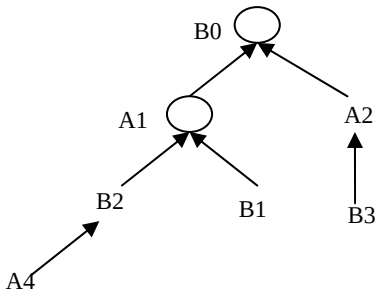


Fig.5. Example of Disclosure Tree

The conversion process from disclosure tree to disclosure sequence is a bottom-up process. From example of Fig.5, trust credential interaction sequence (disclosure sequence) of A and B is {A4,(B2,B3),A2,B1,A1,B0}.Disclosure sequence can arrive at root node B0 via bottom-up converse process of disclosure tree. If disclosure sequence can achieve B0, then it means that trust interaction process of two sides is successful. In fact, different disclosure sequences may be mapped to the same disclosure tree. For example, disclosure tree in Fig.5 has another disclosure sequence {A4,(B1,B2,B3),(A1,A2),B0}.

5. NEGOTIATION PROTOCOL

Suppose that A represents grid service demander, B represents grid service provider. A and B are mutual unknown before. ATN protocol comprises the following specific steps:

(1) A asks for B to request grid service.
(2) B suggests automated trust negotiation. B

promulgates grid service precondition to A; then A promulgates the precondition of this grid service precondition to A. Then A and B interact and exchange trust credential until A and B both satisfies the mutual trust credential requirement. If A or B can not satisfy the mutual trust credential requirement, then the process of ATN is failure.

(3) In term of required trust credentials and policy sets, the disclosure graph is generated, and then the redundant disclosure tree is constructed.
(4) According to the redundant disclosure tree, two sides negotiate a disclosure sequence.
(5) In term of the sequences of disclosure sequence, one side of A and B sends mutual required trust credentials to the other side alternately. Then A and B enter into mutual trust state.
(6) After mutual trust between A and B, B agrees to grid service request from A, then two sides enter into grid service interaction phase.

According to this negotiation protocol, the specific interactive steps of the above example are described:

(1) A asks for B to request grid service.
(2) B promulgates grid service precondition $B0 \leftarrow (A1 \wedge A2) \vee A5$ to A.
(3) There is no trust credential A5, but A1 and A2 in domain A. Then B promulgates preconditions $A1 \leftarrow B1 \wedge B2$ and $A2 \leftarrow B3$ to A.
(4) Domain B encompasses rules $B1 \leftarrow A2$, $B2 \leftarrow A4$ and $B3 \leftarrow TRUE$ .Because the preconditions of B encompass credential A2, B promulgates precondition $B2 \leftarrow A4$ to A.
(5) B brings forward Disclosure Sequence {A4,(B2,B3),A2,B1,A1,B0} to A.
(6) A sends credential A4 to B.
(7) B sends credential B2 and B3 to A.
(8) A sends credential A2 to B.
(9) B sends credential B1 to A.
(10) A sends credential A1 to B.
(11) B sends credential B0 to A, which means that B has agreed to grid service request from A.
(12) A and B enter into grid service interaction phase.

6. CONCLUSIONS

Automated trust negotiation (ATN) is an approach which establishes trust between strangers through the bilateral, iterative disclosure of digital credentials. In this paper, we mainly discuss how to extend the grid security function to provide better support for the dynamic and cross-organizational aspects of Grid activities, by adding facilities for dynamic establishment of trust between parties. We advance the concept of disclosure graph, linking many non-redundant disclosure trees into a single graph, which improve Method Yu.

REFERENCES

[1] Basney J, Nejdl W, Olmedilla D, Welch V. Winslett M. “Negotiating trust on the grid”. *Proceedings Semantics in P2P and Grid Computing at the Thirteenth International World Wide Web Conference*, 2004.
[2] Irwin K, Yu T. “Preventing attribute information leakage in automated trust negotiation”. *ACM Conference on Computer and Communications Security* 2005: 36-45.
[3] Barlow T, Hess A, Seamons KE. “Trust negotiation in electronic markets”. *Proceedings of 8th Research Symposium in Emerging Electronic Markets, Maastricht, Netherlands*, 2001.
[4] Nejdl W, Olmedilla D, Winslett M. “PeerTrust: Automated trust negotiation for peers on the Semantic Web”. *Proceedings of the Workshop on Secure Data Management in a Connected World (SDM'04).LNCS 3178, Springer*, 2004. 118-132.
[5] Yu T, Winslett M, Seamons KE. “Interoperable strategies in automated trust negotiation”. *Proceedings of the 8th ACM conference on Computer and Communications Security*. New York, ACM Press, 2001: 146-155.

Hongwei Chen (1975-), male, from Hubei Province, PHD, Lecturer of Hubei University of Technology, interested in Grid Computing, Peer-to-Peer, Information Security, Mobile Agent.

Research of Security Scheme of EPONS*

Tie Li [1], Li Wang [2], Chuanqing Cheng[1]
[1] Computer Science Department, Wuhan University of Science and Engineering
[2] School of Telecommunication, Wuhan University
Email: wl3833@126.com

ABSTRACT

An EPON.which is going on standardization in IEEE 802.3ah, consists of a OLT and multiple ONU using passive optical components. So this network is susceptible to variable security threats such as eavesdropping, masquerading, denial of service and so on .In this paper we propose the security model of triple churning o support date encryption and decryption to avoid other onu receives other onu's information in EPON based optical access network. We analyze security models in EPON reference model. This paper introduce the churning and de-Churning scheme, include the single churning and the triple churning, the detail of the key message mutual process and the key update process.

Keywords: EPON, Security,Churing, Encryption, Optical Access Network.

1. INTRODUCTION

Several alternatives based either on wired or wireless infrastructure is considered for the provision of broadcast services in the local loops. In the field of wired solutions, Passive Optical Networks (PON) looks very promising one due to their bandwidth capacity.

There are several kinds of PONs, such as ATM-PON, EPON, GPON, WDM-PON, and etc. These PONs are based on shared-medium network. So, they have several security threats.

The EPON consists of an Optical Line Termination (OLT), multiple Optical Network Units (ONUs) and an Optical distribution Network (ODN) with passive optical components. The EPON is a tree topology connecting an OLT with multiple ONUs via an optical link. All transmissions in the EPON are performed between an OLT and ONUS. In the downstream direction, the EPON is a point-to-multipoint network and in the upstream direction, it is multipoint-to-point network.
On the downstream direction, an OLT broadcasts the information to all ONUs. Every ONU can drop downstream traffic unnoticed. ONUs share the upstream channel capacity and network resources. Therefore, the EPON is exposed some threats about data security. In this paper, we analyze security vulnerability and position of security service in the EPON reference model. We discuss the key problems of the security of EPONs , then introduce the churning scheme, include single churning and triple churning. The key message mutual process and the key update process is introduced in detail.
The rest of this paper is organized as follows. In section 2, we analyze security problems of the EPONs, point out that the downstream broadcast is a great security problem. We present the churning and de-churning scheme in section 3. In section 4, we describe the key mutual message. Section 5 discussed the key update process and the section 6 conclusion the paper.

2. SECURITY OF EPONs

On the downstream direction, an OLT broadcasts the information to all ONUs in EPON system. It is easy for hacker to capture other user's information, just as the Fig. 1 showing. On one hand, the hacker can wiretap the personal information of others .On the other hand, he can intercept and capture the downstream control frame and OAM frame to get the authentication and network management information. The security of EPON is one of the most noticeable problems for service supplier.

churning provides the necessary function of data scrambling and to offer protection for data confidentiality .Deploying downstream churning and de-churning, EPON system can assure isolating user's information, the downstream information only can be received by destination ONU. Deploying upstream OAM frame or MAC control frame, EPON system can prevent hacker fabricating OAM frame or MAC control frame and to modify system configuration and even to destroy the system.

Moreover China Telecommunication advise to deploy triple churning. On downstream direction, the churning will be done to each LLID's data. Each LLID has its own key. The OLT starts the key refresh demand, the ONU supplies the key and OLT finished churning function by the key. After start churning, all the downstream data and the OAM frame will be churninged. The key refresh and synchronization process will deploy the extended OAM PDU frame which is open to all the device corporation.

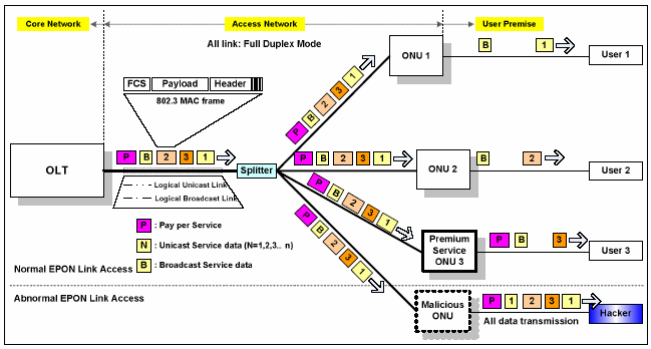


Fig.1. EPON security

* This work is supported by Hubei Province Natural Science Foundation under Grant 2006ABA296

3. CHURNING AND DECHURNING

To improving data security, EPON system should use the triple churning method .The triple churning method is a extension of single churning and increase the data time relevance to improve the security of user's data.

3.1 Single Churning

The churning algorithm regulated by G.983 is: use the 3 bytes(X1-X8,P1-P16) random number as churning code, then use the algorithm to generate the assistant churning parameter K1-K10.The 34 bits consist of a group churning keys. At the churning side, make churning with 18bits (P1-P8 and K1-K10) to 8bits width data. At the De-churning side, make de-churning with the 18bits to the 8bits width data.

As the cryptography principia, the encryption algorithm is public and the key is secretive. Encryption and decryption uses the same key. OLT and ONU assure key synchronization by handshake. The key is requested by OLT and generated by ONU.

The churning start from the destination MAC filed of Ethernet frame, and end at the FCS filed. After finishing MPCP discovery and OAM discovery, the switch of churning key begins. Then all the downstream data frame, MAC control and OAM frame should be churninged.

The Key K1-K10 generated as the logic:
K1 = (X1*P13*P14) + (X2*P13*not P14) + (X7*not P13*P14) + (X8*not P13*not P14)
K2 = (X3*P15*P16) + (X4*P15*not P16) + (X5*not P15*P16) + (X6*not P15*not P16)
K3 = (K1*P9) + (K2*not P9)
K4 = (K1*not P9) + (K2*P9)
K5 = (K1*P10) + (K2*not P10)
K6 = (K1*not P10) + (K2*P10)
K7 = (K1*P11) + (K2*not P11)
K8 = (K1*not P11) + (K2*P11)
K9 = (K1*P12) + (K2*not P12)
K10 = (K1*not P12) + (K2*P12)

3.2 Triple Churning

Triple churning uses three cascade connected churning. Each churning implement the churning function as 3.1.The key of each churning is different. The first churning uses the primordial 24bits key(P16-P1,X8-X1), the second churning uses the key which is right shifted 1 byte by primordial key(X8-X1,P16-P1), The third churning uses the key which is right shifted 2 bytes by primordial key (P8-P1,X8-X1,P16-P9).The first churning_1's output bit XOR the two 8bits vectors .The first vector is the previous input encryption byte, when the byte is the first encryption byte of the data frame, the vector is the lowest bit of the key. The second vector is the former four bytes's triple churning output. The method can make the current churning output have some relation with the former churning output, so the shortage of single churning that some figure appears repeatedly will not be detected by triple churning.

The XOR result XOR1 bit shift as some rules to input churning2.The rule is like the following: the bit2 and bit4 swaps, bit3 and bit5 swaps, bit0,1,6,7 is remain with no changes. As the following figure:

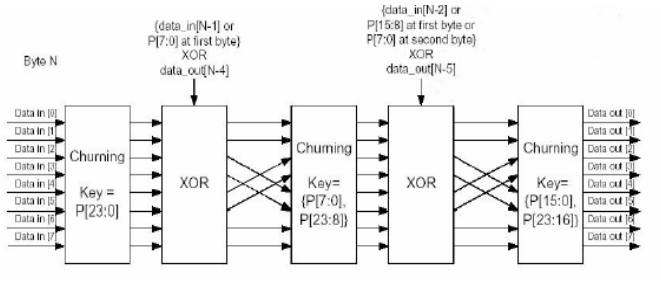


Fig.2. Triple churning

The second churning engine churning_2's output bit XOR two vectors too. The first vector is the former two bytes input encryption byte. When the byte is the first encryption byte, the vector is the second low byte. When the byte is the second encryption byte of a frame, the vector is the lowest byte of the key. The second vector is the triple churning output of the former 5 bytes.

The output of XOR_2 still bit shift and input to the third churning engine. The shift rule is like the former.

4. KEY MUTUAL MESSAGE

The key mutual message for churning include four types:

- New key request frame
- New churning key frame
- New churning key update frame
- New key active frame

The four messages can be transmitted by OAM frame. The OAM frame must be extension to add the organization-specific information.

The ordinary OAM PDU is as the following:

Table 1. Ordinary OAM PDU

Preamble	2
DA	6
SA	6
Length/Type	2(0x8809)
SubType	1(0x03)
Flags	2
code	1
Data/Pad	42-1096
FCS	4

By means of setting the code field to be a specific value to indicate that the frame is the organization-specific extension PDU. Then the part of payload is just like table2:

Table 2. Ordinary OAM PDU

3	OUI
1	Message type(churning)
1	-Churning message, New key request -Churning message, New churning key -Churning message, New churning key update -Churning message, New key active frame Reserved Ignored reception

5. KEY UPDATE PROCESS

The key refresh process includes new key request frame and new churning key frame. OLT send new key request frame to ONU.ONU send a new churning key frame back to OLT.
The key synchronization is implemented by churning key update frame and the churning key active frame. When the OLT receives the new churning key frame, it sends churning key update frame to ONU. The churning key update frame includes two parameters: key id and new key take effective time. The key-take-effective time means the time of new key to take effective. The relation time interval between the time and the sending time of the frame is time shift(Tshift). The key ID means the current mutual key ID. Since the churning key update frame brings the time tag and the key ID, when the ONU receives the frame, it will know the time at which OLT starts to use the new key. Because the local time register of ONU is in step with the frame time mark, so the time is also the start time at which ONU starts to use the new key to decrypt.

When ONU receives the churning key update frame, it sends the churning key active frame to OLT to indicate it accept the key refreshing.If the OLT receives the churning key update frame from ONU, it will use the new key at the delay of Tshift after sending the churning key update frame and indicate that the data is encrypted and the key ID.

Considered the time drift, ONU will start delay Tshift-8TQ after receiving the first churning key update frame .If the received frame is a encryption frame and the Key_Index is equal to the key ID in the churning key update frame, the ONU decrypt by new key, or by old key. If the OLT does not received churning key active frame at the Tshift after send churning key update frame, it will consider the key mutual failed. OLT send new key request frame again. Before succeed in new key mutual, the OLT still uses the old key and send the information to network manager.

The new key take effective time in new key request frame and the Tshift and the key refresh time Tkey can be configured. The key refresh and synchronization is like Fig.3:

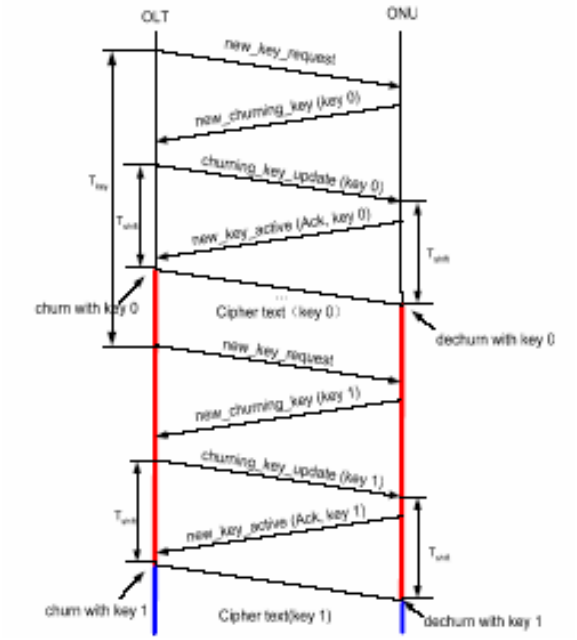


Fig.3. Key refresh and synchronization

6. CONCLUSIONS

The transmission characteristics of EPON where downstream traffics are broadcasted from an OLT introduces security vulnerabilities and threats such as eavesdropping, impersonation and denial of service. In this paper we introduce the triple churning to avoid the security problem. Churning and de-churning of EPON downstream data frame and the upstream OAM frame has advantages to protect against traffic analyzing, OAM traffic hacking, and MPCP message eavesdropping. A full scheme of the security, include the message format, message mutual process and the key update process is introduced in detail. Except for this, the security of EPON also come down to MAC address amount limit, broadcast and multicast frame control, user uniqueness and etc. For cosmically applied and spread, the security of EPON will be more attractive attentions.

REFERENCES

[1] http://www.c114.net/technic/technicread.asp?articleid=397 [2]*IEEE* 802.”3ah Ethernet in the First Mile Task Force”.
[2] *IEEE* Std 802.1~-2001: “Port-Based Network Access Control”.
[3] WilliamStallings, “Cryptography and Network Security,”2nd Edition, Prentice-Hall, 1999
[4] Sun-Sik Roh, “Security Model and Authentication Protocol in EPON-based Optical Access Network,”*ICTON2003*
[5] Jee-Sook Eun, “The Design of Key Security in Ethernet PON,”*ICACT2006*
[6] Kyeong-Soo Han, “The Design and Implementation of MAC Security in EPON,”*ICACT2006*
[7] “Analysis and assure of security about MS-EPON”, http://www.host01.com/Print.html?53793,1
[8] CTC. “EPON device technology demand”.

Tie Li is a vice-professor of Wuhan University of Science Technology. He has published one bookes, over 10 journal papers and many o f which is indexed by EI or, ISTP. His research interests are in distributed parallel processing, grid computing, network security and e-commence.

Analysis and Research of Win32 PE Virus Polymorphism

Sheming Gao[1], Qiang Xiong [1], Lina Lu [2]
[1] School of Computer, Wuhan Univ.of Techn., Wuhan 430070, China
[2] Computer teaching and research section, Basic courses department, Wuhan Ordnance Non-commissioned Officers Academy, Wuhan 430075, China
Email: Xiongqiang8101@163.com

ABSTRCT

With the development of Virus technology, more and more Virus realized polymorph by the encryption and deformation techniques which make the traditional scan technology feature codes lost its function and improve their survival ability in infected OS.

Keywords: Win32 PE Virus, Encrypt, Polymorph Engine

1. INTRODUCTION

Of all the viruses, win32 PE virus is the most numerous and devastating one. At the earlier time, the scanning technology based on attribute code was quite effective in defending against this virus .however, more and more viruses have adopted distorting encoding technology to improve their surviving chances in infected computers. The traditional attribute code scanning technology is powerless towards them. Usually, the viruses that would not be detected by ordinary attribute code scanning technology are called polymorphism. The detection-proof technology adopted by polymorphism mainly includes two aspects: making use of unfixed codes or random encrypting codes, or changing the virus codes while it is functioning.

2. PRINCIPLES OF THE WIN32 PE VIRUS

The common way of PE virus to infected other documents is to add the new code and the codes which returns to the host procedure after the viral execution, and revises the enter code which carry out the position (Address of Entry point) to point to the new added new byte, in order to carry out the new code after the procedure movement. Here is the analysis of the general process of the document infection below [1]:

1) Check the start two bytes are the "MZ" of the object document.
2) Check the document PE signed "PE".
3) Checks the infection sign, if it has been infected, exit from continue the HOST system, if not, continue.
4) Try to get the number (each data catalog has eight bytes) of the Directory (data catalog).
5) Obtains the start place of section table (offset address of Directory+ the number of bytes which are occupied by the data catalog=the start position of byte).
6) Obtains the foot offset of the present final section table's.
7) Start to read in the section table:a.read in the section name(eight bytes);b. the achieved byte number read in section(four bytes);c. read in the start offset address in EMS memory of new section(four bytes),also calculates the entrance position of the virus. The up section start offset address in memory+ (the magnitude of up section/align at section+1) align at section=the start skewing address of section in memory; d. read in this section (virus byte) magnitude after align at the byte; reads the start position of this section in file. the up section start address in files+ the magnitude of up section align at in files=this section (virus) start position in document; f. revamp the number of section table in reflection of begin-of –file; g. while revamp the Address of Entry point (the procedure entrance point to the virus entrance position), save the old Address of Entry point, convenient for return the HOST continue to carry out; h. update the Size of image (the whole PE reflection dimension=former
8) Size of image+ the magnitude of virus section after memory justification); i. read in the infection sign (the follow example is put in front of the PE); J. read the virus code into the new section: ECX=virus length;ESI=virus code position(it is not equal with the start position if virus carry out code);EDI=virus section position(the follow example is the correspond position in memory reflection document);k. setting the current document position for the end document.

These kind viruses which can easily insert to the PE document commonly have root feature code, it based on the static state scanning technique of feature code can resist this kind of virus effectively.

3. ENCRYPTION OF VIRUS AND ANALYSIS OF POLYMORPHISM TECHNOLOGY

3.1 The Analysis of Encrypted Virus

In order to confront the scanning technology of static state code, some virus will first encrypt the code of virus and carrying on the process of decipher. The features of these viruses are: there is a decryptor at the entrance; and the code of virus is encrypted. When running the application the decipher code which get the masterdom will decipher the virus in circulation and then transmit the masterdom to the virus. When infecting a document, the virus will write the decryptor together with virus which be encrypted stochastically by the key and the key which be kept or embed in decryptor into the infected document. Following is a simply encrypted virus diagram. See Fig. 1:

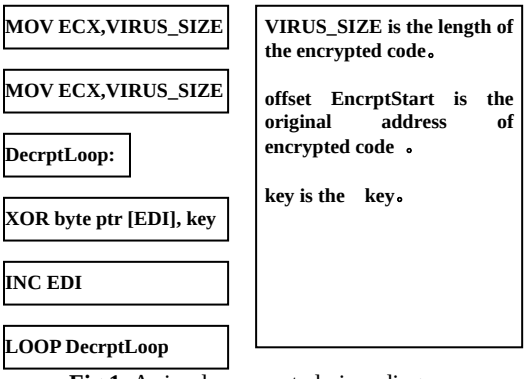


Fig.1. A simply encrypted virus diagram

As for the same virus in different infection cases, it is encrypted by different keys, so it is impossible to find an only section of code string and offset of the virus to represent the features. But in different infection cases, the decryptor has the same definite orders of machine code. So, when dealing with the viruses of this kind the traditional technology of static state code scanning can still do.

3.2 The Analysis of Deformed Polymorph Virus

As the encrypted virus can not escape thoroughly from scanning of characteristic code in static state, the writer could improve the virus on the base of the encrypted one to make the code of decryptor presenting multiplicity in different infection cases, so there comes encrypted polymorph virus [2]. It is very similar with the encrypted virus. The only improvement of it lies in when infecting different documents the virus could structured different coded decryptor with the same function, that is to say, in different cases, the decryptors have the same deciphering function but a totally different code. The codes which help realizing the polymorph deformation of decryptor is called polymorph engine. A polymorph engine should consist of modules as follows: module of stochastic register choice, module of stochastic value choice, module of instruction generation, module of trash code generation. The following is a frame of polymorph engine generated by the combined employing of those modules. See Fig. 2.

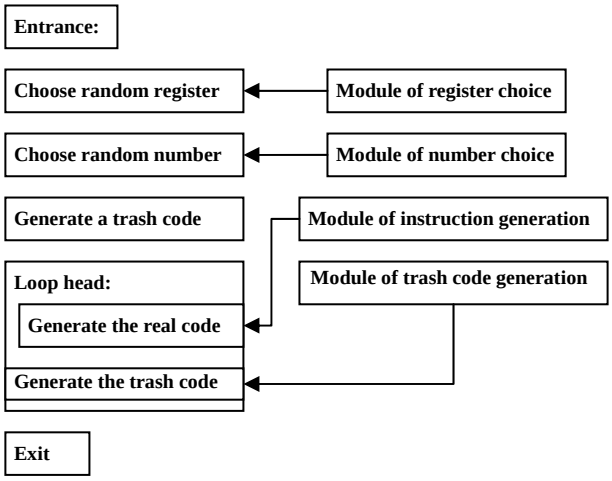


Fig.2. A frame of polymorph engine

Under the instruction of the diagram, we could write a section of concept polymorph virus which could first decipher the encrypted virus and then jump into the function of infecting and destructing the virus code. See Fig. 3.

This section of decipher code and encrypted virus are both generated stochastically when infected. The register, key, the length of encrypted data and even the instructions are stochastic. So the whole virus data have no fixed virus characteristic code. The traditional technology of static state characteristic codes scanning lose its effect when dealing with those encrypted polymorph virus. But after being deciphered, the definite orders of virus become stable. As long as getting the deciphered virus, we could scan by using the characteristic code. If we want get definite orders of virus, we should first employ virtual machine to explain the decipher of the virus.

code	Explanatory notes
MOV reg_1,count **MOV reg_2,key** **MOV reg_3,offset** **LOOP** **XXX byte ptr[reg_3],reg_2** **DEC reg_1** **JXX LOOP** **Code of encrypted virus**	**Among those codes, reg_1 is a register chosen stochastically from AX, BX, CX, DX, which was infected by different documents. Decipher code employ the stochastic register. Count is the length of encrypted data. Key is the encrypted cipher code. Offset is the offset of the encrypted data. When effected, those data are generated by stochastic data. XXX is general designation of many different operation instructions like XOR, ADD, SUB, etc. JXX is the general designation of those jumping instructions such as JA, JNC, which is generated stochastically by generation modules when operating.**

Fig.3. The virus code

4. CONCLUSIONS

The thesis analyzes the infection process of the simple win32PE virus. These viruses generally written by win32 assembly language which has its own advantages such as using nimbly, could controlling the low layer of the system, and the volume of the generated code s small and easy to hide. Only after analysis the mechanism, key technology and infection process of the virus, we could explain and control it.

REFERENCES

[1] Chen.L.C.,Carley.K.M.The Impact of Countermeasure Propagation on the Prevalence of Computer Viruses.System,Man and Cybernetics, Part B, *IEEE Transactions on,Volume:34,Issue:2,April 2007.*

[2] Leitold," F.Mathematical Model of Computer Viruses, "*EICAR 2000 Best Paper Proceedings.*

Neural Network Computing

Fault Diagnosis Based on Neural Network Expert System for ATM Network*

Yongjian Yang, Yongjun Pan
College of Computer Science and Technology, Jilin University
Changchun, Jilin, 130012, P.R.China
Email: yyj@jlu.edu.cn

ABSTRACT

With the characteristics of high speed, large information, and complex running parameters, the ATM network needs the support of intelligent management system to analyze network faults. It's proposed that we can use the ideas of neural network expert system to manage the faults of ATM network in this paper. We make use of BP neural network model whose performance is comparably stable in order to improve the convergence speed of fault diagnosis. On the other hand, we build up the expert system using production rule knowledge form which is widely popular, so that we can diagnose the ATM network faults intelligently and mange them effectively.

Keywords: Fault Diagnosis, Neural Network, Expert System, ATM Network

1. INTRODUCTION

Fault management is an important part of ATM network system management, and fault diagnosis is the basis of fault management. For the management of ATM network, the data is large, the correlation is complex, the demand of real-time on line is high, the structure and arrangement are also complex, and the same network fault maybe has different predictions, or the same prediction may result in different faults. This brings difficulties for analyzing and locating network faults. It's fit for fulfilling intelligent management using expert system [1]. Moreover, the network watching needs to deal with large data, and these data is always incomplete, discontinuous and irregular in ATM network. The parallel processing is suitable for this. In this paper, we bind the expert system and neural network together to diagnose the ATM network intelligently, so that we can make artificial intelligence more useful in ATM network fault diagnosis.

2. IMPROVEMENT OF NEURAL NETWORK MODEL

2.1 Multi-layered Feed-forward Neural Network

There are many kinds of neural network models at present and each one has its own practice field. It's showed in many experiments that the performance of fault diagnosis in BP neural network is better [2][3].

BP neural network model is a kind of multi-layered feed-forward network [4][5]. It employs error back propagation algorithm to make the network study convergent. There are three kinds of nodes in BP network: input layer nodes, hidden layer nodes and output layer nodes. The input signal is first propagated to the hidden layer nodes and handled by the function, and then the output of hidden node is propagated to the output node or next hidden node. In the end, the output node produces the results. If the output isn't desired, the error back propagation process will run. The error signal will be propagated back, and it will get smaller via modifying the weights and thresholds of neurons in each layer. With the alternation processes of "forward propagation" and "error back propagation" over and over again, the actual output of network is approaching the desired output, implying that the correctness rate of network responding to input is rising.

BP network can be regarded as a nonlinear function mapping input onto output [6]. H: any given continuous function, f: U_n->R_m, f(X)=Y, U is [0,1]. f can be realized with a three-layered feed-forward network accurately, in which the first layer has n process units, the second layer has 2n+1 , and the third layer(output layer) has m ones.

The three-layered neural network model used in this paper is depicted as Fig.1.

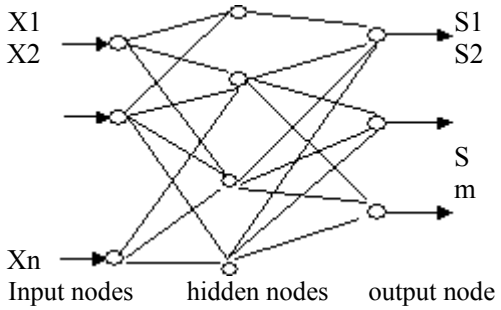


Fig.1. three-layered neural network model

2.2 BP Neural Network Algorithm and the Improved Model

The main idea of BP algorithm is modifying the errors when propagating them back to adjust the network parameters (weights, thresholds), so that it can realize or approach the desired mapping input onto output. It does two transmitting calculations in each training.

(1) Initialize the weights vector W and threshold θ determining the state of network with the smallest random number.

(2) Input a sample vector X as the input signal of the network.

(3) Consider the input vector X as the output vector I of the input layer, and calculate the sum of input and output signals of each node in the middle layer. For example, node j of the middle layer will calculate:

$$U_j = \sum_i W_{ji} \cdot I_i - \theta_j \quad (1)$$

$$H_j = f(U_j) \quad (2)$$

(4) Calculate the sum of input and output signals of each node in the output layer as before. For example, node K will calculate:

$$S_k = \sum_j W_{kj} \cdot H_j - \theta_k \quad (3)$$

$$O_k = f(Sk) \quad (4)$$

(5) Calculate the error δ of each node in the output layer employing the input sample vector X and the corresponding teacher vector T. For example, the δ_K of node K is:

$$\delta_K = (O_K - T_K) \cdot O_K \cdot (1 - O_K) \quad (5)$$

* This paper is supported by the key science and technology developing and researching subject of the Ministry of Information Industry (98046).

(6) Calculate the error vector δj of each node in the middle layer employing error vector δ and the weight vector W from the middle layer to the output layer.

$$\boldsymbol{\delta}_j = (\sum_K \delta_K W_{kj}) \times H_j \cdot (1 - H_j) \quad (6)$$

(7) Correct the weight vector W of the output layer and the middle layer, and the threshold vector θof nodes in the output layer using the result error vector δ of (5). For example, the W_{kj} connecting the nodes K and J, and the threshold of K, θ_K are corrected:

$$W_{kj} = W_{kj} + \alpha \cdot \delta_K \cdot H_j \quad (7)$$

$$\boldsymbol{\theta}_K = \theta_K + \beta \cdot \delta_K \quad (8)$$

(8) Correct the weight vector W of the middle layer and the input layer, and the threshold vector θ of the nodes in the middle layer using the result error vector δ of (6). For example, the Wkj connecting the nodes J and K, and the threshold of J are corrected:

$$W_{ji} = W_{ji} + \alpha \cdot \delta_J \cdot I_i \quad (9)$$

$$\theta_j = \theta_j + \beta \cdot \delta_j \quad (10)$$

(9) If the error vector is below the given vector, store the latest weight value and threshold. Setting a minimum of error is to prevent from librating.

(10) If there is study sample not being taken, take the next study sample as the input vector and return.

(11) If all of the study samples are taken, update the times of study. If it is in the limit of study times, return.

(12) It's up to the study times, and the study process ends.

BP algorithm has many advantages such as clear reasoning and high study precision. But in BP algorithm, the convergence speed is so slow as several thousand or even more steps, and what's more, it's probably not convergent. The cause of slow convergence is that error is nonlinear function of the time, while BP algorithm is employing maximum gradient reducing algorithm, and the weights are modified in the smaller direction of partial derivatives of error to weight. When approaching convergence, f'(x)=0, and the convergence is slow. The initialization value is a small random number, and weight increment:

$$\triangle W_{ij} = \eta \delta_i X'_i \quad (11)$$

In this formula, each coefficient has different corrective degree. But η is keep constant, which maybe lead to over correctness. So only when η is small it will convergent.

In order to improve the convergence speed of BP algorithm, we take measures as follows:

1) Use variable step size. Adjust the study coefficient automatically and gradually. After a cycle of study sample, we calculate error increment:

$$\triangle E = E(i) - E(i-1) \quad (12)$$

step size increment:

$$\triangle \eta = -\beta \triangle E \quad (13)$$

here,

$$E(i) = \{ [\sum_{k=1}^{m} (Tk(i) - Oki))] / m \} \cdot N \quad (14)$$

N is the number of study samples

β<1, and is a constant. When △E>0, reduce the step size; when △E<0, increase the step size.

2) Modify stimulant function f(X):

$$f(x) = (1+2\alpha) / (1+\exp(-x)) \quad (15)$$

αis a constant whose value is below 1. When f(x)=0, x≠0, and the convergence is speeded up. Obviously, the larger α is, the faster convergence is, but it's easy to result in librating. So, αneeds to be chosen suitable.

3) Add momentum value

$$W_{kj} = \alpha \cdot W_{kj} + \eta \cdot \delta_k \cdot H_j \quad (16)$$

α is called momentum value, and is a positive number. It can play the role of stabilizing and adjusting.

After the three steps above, the BP algorithm is improved and the convergence speed is higher.

3. PRACTICE OF FAULT DIAGNOSIS

In order to realize fault diagnosis of neural network expert system, at first, we extract data from ATM switchboard, and then diagnose. In the process of diagnosis, search the corresponding premise in the rule base of the expert system. If find, output the result of diagnosis directly; or else, diagnose the result employing the self-study function of neural network. After the user affirms the diagnosis result, it begins self-study and adjusts the weights and threshold of the system to make diagnosis more accurate.

3.1 Data Extraction

Extract the data from ATM switchboard, mainly the port of ATM switchboard, the data rate of input and output and sum from this port, the error rate and loss rate of data packages input and output from this port, record time and so on.

3.2 Build up the Expert System Knowledge Base

We represent expert knowledge using rule-based production method. Production rule consists of premise and conclusion, and is easy to realize with the table structure RULE in database. In RULE table, the premise of rule contains 4 fields, which are the error rate of input and output data packages, the loss rate of input and output data packages; while the conclusion contains 7 fields, which represent the reasons of network faults naming diagnosis results now.

In our system, we make use of forward reasoning with data driver to diagnose the fault type directly through the input data. What's more, we employ the self-study of neural network. In the process of running, the network is gradually expanding its knowledge base in each diagnosis. Before the system runs, there is some expert knowledge stored in the rule base in order to be used in neural network training.

3.3 Network Training

In our system, we need to initialize the weights and thresholds, and then train to adjust them as to ensure the result correct. The flow of program is as Fig.2.

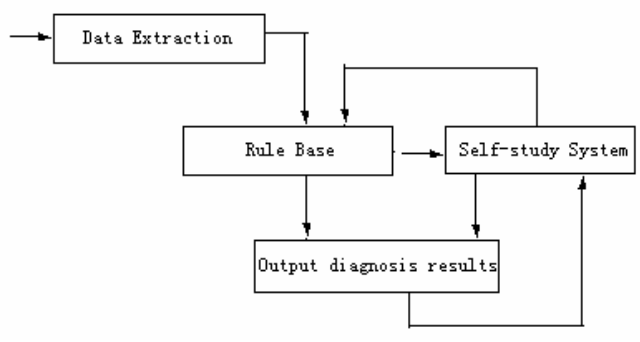


Fig.2. Network Training flow of program

We use the improved BP neural network model, in which the characteristic curve of neuron is a sigmoidal nonlinearity function: f = 1/(1+exp(x)); the study rule is error-correcting rule, that is altering the weights based on the outward response from the output nodes; while the reasoning process is number calculation.

Take the premise in the RULE table as input signal of the input

nodes, and the possible causes of each fault as the output value. Then the input layer has 4 neurons, according to Kolmogorov theorem, the hidden layer has 9 neurons and the output layer has 7 ones.

The network training plays an import part in the whole system because study process is built up with the building of knowledge base. When choosing the study samples, we should pay attention to the use of typical samples and actual samples. The former can stand out the characteristics of the network faults, and can make concepts and extract characteristics more quickly. The latter can show the personal characteristics of the equipment more clearly, and improve the fault-tolerating capability employing the information it takes.

In the process of training, the main task is altering the weights and threshold on the base of the original values to ensure the network keep balance and the diagnosis result be correct. According to the study samples above, in the usual algorithm, the times of network training is more than 3500. While in the improved BP algorithm, we can get better network model in which with the times increasing, the mean error of the network is reducing gradually at high speed. In other words, the improved algorithm has higher convergence speed and precision.

3.4 Fault Prediction and Determination

Once finishing training, the neural network can not only diagnose the faults found before, but can also diagnose the analogous faults never found. In the process of diagnosing, according to the extracted data (the input variable embodying the fault prediction), at first search the rule base of the expert system, if find the corresponding rule, output the result directly; or else, use the diagnosis of the neural network. The diagnosis process is as Fig.3.

For example, the kinds of faults and the probable causes are as table 1.

According to the above table, after getting the fault conclusion, through referencing the probable cause, we can get rid of the fault quickly

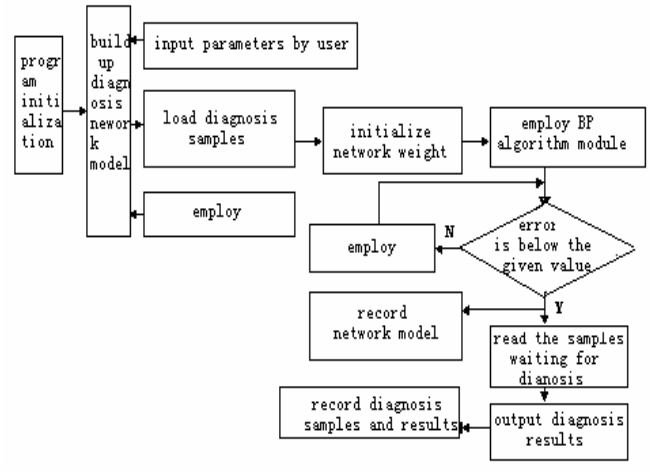


Fig.3. diagnosis process flow

Table 1. Kinds of faults and the probable causes

Fault kind	Fault conclusions	Probable cause
Fault 1	Network circuitry is abnormal	The circuitry is seriously disturbed by electromagnetism
Fault 2	Ethernet repeaters is abnormal	Repeater is broken
Fault 3	Router interface is broken	CPU of router is over-loaded，and EMS memory has little free
Fault 4	Physical circuitry problem	The equipment of circuitry is broken, the pin is loose
Fault 5	Network running problem	The data buffer overflow, or receive unsupported protocol packages
Fault 6	Software of logic problem	Important process or port is shut down
Fault 7	Route fail	The router port parameter is error route mask is error

4. CONCLUSIONS

This paper is a result of an important technique development project of Ministry of Information Industry. It is also a production of ATM network maintenance and prevent-control expert system. Meanwhile, it's a successful attempting of using neural network expert system in ATM network fault diagnosis. The characteristics of ATM network determine that its fault diagnosis should be real-time. The data gathered in this system is extracted from MIB base of ATM switchboard, and after several improvements of BP algorithm, the convergence speed is very high, implying that the fault diagnosis is more practicable and intelligent.

In order to find the network faults in time and reduce the loss due to faults, we add the functions of real-time watching and warning in this system. When there is serious mistake, sound the bell to alert the network manager. When the mistake rate of data packages reaches the threshold, the warning is going on, until someone deals with it, and then the work will continue.

REFERENCES

[1] Yongjian Yang, Songyang Han: "Expert System Intelligent Management For ATM Network" *IEEE SMC'99 conference Japan* 1999-10

[2] Feng Liu, Chunxian Xia, Zhenhe Huang: "Fault diagnosis expert system based on artificial neural network" *Foreign Electronic Measurement Technology* 2004 Volumn.04

[3] Jiazhou He, Zhihua Zhou, Yang Gao, Shifu Chen: "Fault diagnosis model based on new neural network classifier" *Journal of Computer Research and Development* 2001 volume.01

[4] "Pap RM.Neural networks based fault diagnosis for the NASP." http://www.accurateautomation.com/contract/

[5] Yafeng meng, Jinyan Cai, XianBing Cao: "Radar fault diagnosis based on neural network" *Chinese Journal of*

Science Instrument 2003 Vol. S1
[6] Yanghong Tan, Yigang He, Hongyun Chen, Jie Wu: "Fault d iagnosis neural network method of large-scale circuit" Journal *of Circuits and Systems* 2001 volumn.04.

Yongjian Yang is a Full Professor of Computer College, the vice Dean of Software College in Jilin University. He is also a Committeeman of Directing Committee for Computer Teaching of National Education Ministry, the Director of Key Laboratory of Computer Communications of Ministry of Information Industry, and a syndic of Computer Academy of Jilin Province. He received the master degree of Computer Application from Beijing University of Posts and Telecommunications and Ph.D degree of Computer Application from Jilin University. He has been studying Computer Network Communications. He has presided more than 10 important projects, and published 2 book and over 50 journal papers.

Research on Remaining Pre-Stress of Diseased Pre-Stressed Concrete Bridges Based on Neural Network*

Xiongjun He[1,2], Xiaojun Che[2], Guohua Hu[3], Mingzheng Cai[3]
[1]Department of Bridge Engineering, Tongji University, Shanghai 200092, China;
[2]Transportation school, Wuhan University of Technology, Wuhan 430063, China;
[3]Road-bridge Ltd Co. of Hubei Province, Wuhan 430051, China)
Email: hxjwhut@163.com

ABSTRACT

According to experimental record of bridges in use, more and more damage bridges have appeared, and the most common and severe defect is the bridge damage and cracking problem, which has seriously affected the normal usage of bridges. Analyzing the disease cause of defective bridges more effectively and deeply, in order to optimize the design and construction of bridges becomes the urgent problem in the engineering field. The study is based on Zhongxiang Hanjiang River (ZHR) Bridge which is destructed as the largest span bridge in China. According to the design, construction data and experimental record of the bridge, a non-linear mapping function from multiple input data (the deck elevation of each element in destructing) to multiple output data (the change of pre-stress) is constructed within BP neural networks. Based on the theory of continuous function, the convergence is disadvantageous between 0 and 1. The study shows the expected output data between 0.05 and 0.95 are better for convergence. According to the real data of bridge floor line change in process of destruction, the released pre-stresses are recognized, and the real pre-stresses in existence are calculated by scheme of cable design. The study not only offers reliable scientific basis for analyzing the disease cause in the bridges, but also is helpful to design of the bridges having same structural style.

Keywords: Neural Network, Damage Bridge, Pre-stress Identification.

1. INTRODUCTION

Just as other structures, bridges have their own lifespan. If the bridges are not managed and protected well, the lifespan will be reduced, even damage suddenly, which is related with over loss of pre-stress. Many scientists from home and abroad have made wide researches on the relationship between the cause of the damage and the loss of pre-stress [1-3]. However, most of the researches are based on the experience or half-experience, and the thory is not mature because of the randomness and uncertainty of pre-stress loss. So the research and analysis of pre-stress loss can offer the effective evidence to analyze the disease causes and give good advices for design and construction of the same bridge styles.

The study takes the ZHR bridge as an example. By FEM analysis of destruction, the training samples of BP neural network are designed. The input data of BP neural network are the values of line shape change of each stage of destruction calculated by FEM, and the the output data are the released values of pre-stresses. In this way, by the real change of each stage, released values of each cable pre-stress are identified. According to the disposition of steel cables, we can calculate remaining pre-stress of each cable.

*This work was supported by Traffic Technology Foundation of Hubei Province (No: [2003]570、[2006]392)

2. BASIC IDEA OF FEM ANALYSIS OF BRIDGE DESTRUCTION

Based on the completion state of the bridge, we can get the stress, displacement and coordinates values. From this state, we can simulate the destruction of all elements of the bridges one by one in the contrary turn of the construction.

In calculation, if a element is destructed, we can simulate that the forces of the element acts on the remaining structure in the opposite direction in fig.1, which can eliminate the action of the element to the whole structure [1-4].

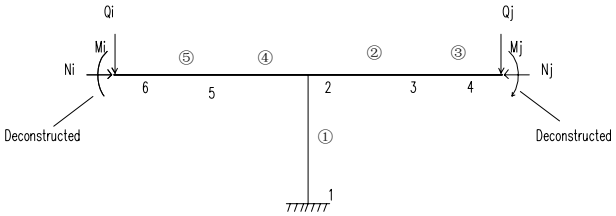


Fig.1. Destruction analysis

Because the calculation of some state is based on the forces and displacements of the previous ending state, to ensure the continuity of the change of forces and displacement and avoid repeated loads, if the loads of previous state do not change in location and value in current state, it will not be reckoned again in this state. While if not, it has to compensate for the changes, and the changes should be added as load increment.

System shift in long-span cantilever construction companies with changing the connecting style, changing the bearing characteristics and canceling or setting up temporary bearing, etc. In order to simplify the input of original data and ensure the continuous process of back-analysis, the bearing, temporary bearing and juncture of elements are simulated as virtual elements in the analysis program.

3. APPROACH TO PRE-STRESS IDENTIFICATION BASED ON BP NEURAL NETWORK

(1) **Setting up sample sets.** For the researched structure, the sample sets of neural network is made up of the floor line shape change of each element, which is acquired through FEM analysis by considering different remaining pre-stress and real concrete intensity of each element;
(2) **Analyzing and selecting sample.** According to the line shape response in the process of destruction, effective

training sample is gotten by orthogonal experiment [5];

(3) **Pretreating data.** Data normalization pretreatment is necessary for the different number level and avoiding the influence to the network study;
(4) Setting up neural network structure for identification of remaining pre-stress and study parameter;
(5) Neural network should be studied until constringency, by taking line shape changes as input data and released pre-stress corresponding to the line shape changes as expected output data;
(6) After successful network study, the effect and spreading capability should be tested by real sample. If error is in a small range, the network study is successful; otherwise it has to be restudied.
(7) For the real structure which is going to be identified, the real line shape changes can be input to the network and the result of which can be real released values of pre-stress in current stage.
(8) By the disposition of pre-stress cables, the remaining pre-stress of each cable can be calculated by adding each value in different procedures step by step.

4. DATA NORMALIZATION OF BP NEURAL NETWORK

Because input data of each joint of BP neural work is quite different, input data normalization has to be done in order to avoid small values submerged by large ones.

According to the continuous function theorem [6-7], the range of input value in network should be in [0, 1]. And for nerve cell which is transferred by the form of Sigmoid function, the range of input value in network should be (0, 1). The experience shows that the function of Sigmoid is bad near 0 and 1, which is disadvantageous to the convergence of network study. So it is good that the expected output data after disposal should be (0.05,0.95) and then input data normalization and output data inverse normalization should be done.

We assume that the sample data is x_p(p=1,2…,n) and define that $x_{max}=\max\{x_p\}$, $x_{min}=\min\{x_p\}$, so the sample can be transferred to the data which is from 0.05 to 0.95 by disposing according to the formula below.

$$x^* = \frac{x_p - x_{min}}{x_{max} - x_{min}} \quad (1)$$

If the transferred function is the form of Purelin[8-9] or Tan-Sigmoid[10] ,the range of function is (-1,1),the disposal of normalization can be done according to the formula below.

$$X^* = 2\frac{x_p - x_{min}}{x_{max} - x_{min}} - 1 \quad (2)$$

Accordingly, output data normalization in network should be done to avoid calculation overflow of the network.

After network study, the output data in network should be reverted, namely verse-transform of normalization. The formulae of verse-transform are formula (3)、(4), respectively for Sigmoid form, Purelin or Tan-Sigmoid form:

$$x_p = (x_{max} - x_{min})X^* + x_{min} \quad (3)$$

$$x_p = \frac{1}{2}(1 + X^*)(x_{max} - x_{min}) + x_{min} \quad (4)$$

5. RECURRENCE FORMULA OF REMAINING PRE-STRESS OF CABLES

Fig.2 shows the release of the top plate cable. we get the analysis process of remaining pre-stress calculation (element K as an example) as follows.

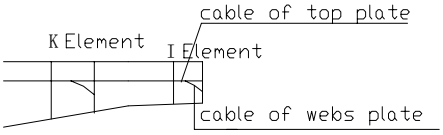


Fig.2. Analysis of Released Pre-Stress of Top Plate Cables

1st procedure (jacking temporary pier):

1st released value of cable S11-S01 can be calculated as $\triangle S_1^k$ (k=1-11) by the method above.

2nd procedure (cutting closure segment, the largest cantilever state):

2nd release value of cable S11-S01 can be calculated as $\triangle S_2^k$ (k=1-11).

3rd procedure (cutting element 11):

3rd release value of cable S_{11}-S_1 can be calculated as $\triangle S_3^k$ (k=1-11).

The remaining pre-stress of S_{11} can be calculated by recurrence as

$$S_{11}=\triangle S_1^{11}+\triangle S_2^{11}+\triangle S_3^{11}$$

The remaining pre-stress of cable S10 can be calculated:

$$S_{10}=\triangle S_1^{10}+\triangle S_2^{10}+\triangle S_3^{10}+\triangle S_4^{10}$$

By analogy, the remaining pre-stress of cable S_9 to S_1 can be calculated as formula （5）:

$$S_k = \sum_{i=1}^{14-k} \Delta S_i^k \quad (5)$$

(k=11-1)

6. ANALYSIS OF THE ENGINEERING

Fig.3 shows FEM model of the 2nd span of the ZHR continuous beam bridge, which has inclined 45 degrees crack along the webs plate in the location of 1/4 of 2nd span, and there is subsidence on the bridge floor.

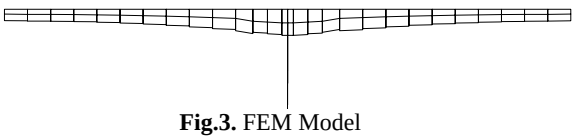


Fig.3. FEM Model

6.1 Process of Calculation

(1) The samples can be made through orthogonal experiment by the line shape changes of the procedures: jacking temporary pier (1st procedure), cutting closure element (2nd procedure) and cutting element 11(3rd procedure) so

that the samples are represented widely. And the remaining pre-stress are taken as 95%, 90%, 85%and 80% of the control stress.

According to the FEM analysis of 12 sample orthogonal design in table 1, which is L24($3^1\times4^1\times2^3$), namely 3 level 1 factor×4 level 1 factor×2 level 3 factor, the line shape changes of element 1-11 can be calculated as input data and output data as released pre-stress of cables in each stage, and then BP neural network can be trained.

Table 1. Orthogonal Experiment (training samples)

Number	stage	pre-stress (%)	Number	stage	pre-stress (%)
1	1	95	7	2	85
2	1	90	8	2	80
3	1	85	9	3	95
4	1	80	10	3	90
5	2	95	11	3	85
6	2	90	12	3	80

(2) After the samples are trained, the released values of pre-stress in each stage can be identified by choosing line shape changes in the destruction as input data, if we choose the released values of pre-stresses of cable S_1-S_{11} fixed on the top plate and the web as research object, the results of identification are as table 2.

6.2 Comparison of Remaining Pre-Stress and Control Stress

Comparison of remaining pre-stress and control stress is showed in fig. 4.

By comparison, we find that the remaining pre-stress of most cables is small, and the loss of pre-stress is over 30%, in which the biggest loss is 47.58%, and load carrying capacity is reduced very much.

7. CONCLUSIONS

According to the analysis above, we set up the nonlinear mapping relationship by using BP neural network from the real line shape changes in destruction to the released values of the destructed cables. In this way, the released values of pre-stress of cables in each stage are identified, and the remaining pre-stress of each cable can be calculated by recurrence. We can draw the conclusions as follows:

(1) It is suggested that the expected input/output of BP neural network after disposal between (0.05, 0.95) be taken to improve the efficiency and convergence rate if the input data is dealt with by normalization, while output data is done by inverse normalization.

(2) Remaining pre-stress has been identified by BP neural network, and according to disposition of the cables, the loss of pre-stress can be calculated, and the real disease cause of this kind of bridge is estimated. The result of identification indicates the method is effective. Not only does the method offer reliable scientific basis for analyzing the disease causes in the bridge, but also it can be realized by designer to avoid the disease causes of the same kind of bridges.

Table 2. Results of Identification of Released Pre-Stress in Each Stage

Number	Stage/ released values of pre-stress of cables in the stage（MPa）												
	jacking temporary pier	cutting closure element	cutting element 11	cutting element 10	cutting element 09	cutting element 08	cutting element 07	cutting element 06	cutting element 05	cutting element 04	cutting element 03	cutting element 02	cutting element 01
S11	118.25	275.32	511.47	—	—	—	—	—	—	—	—	—	—
S10	144.12	145.23	149.23	482.84	—	—	—	—	—	—	—	—	—
S9	129.18	161.32	171.12	187.12	278.38	—	—	—	—	—	—	—	—
S8	62.15	62.35	84.25	98.14	1.0.45	492.42	—	—	—	—	—	—	—
S7	73.16	76.25	78.14	80.26	75.01	138.63	479.98	—	—	—	—	—	—
S6	72.58	72.64	75.12	75.26	75.88	85.62	99.25	131.32	—	—	—	—	—
S5	82.04	85.45	87.65	93.45	93.65	118.65	117.26	139.88	168.15	—	—	—	—
S4	61.95	61.65	62.98	63.04	64.01	64.98	65.02	65.62	72.30	149.07	—	—	—
S3	61.96	64.36	65.68	60.98	61.32	62.65	66.98	63.62	68.12	75.99	250.12	—	—
S2	71.02	71.92	72.01	72.96	73.65	74.02	74.32	74.96	76.25	79.36	93.15	97.08	—
S1	61.00	61.62	62.00	62.95	63.95	64.17	65.32	65.00	68.15	60.14	60.14	63.15	167.84

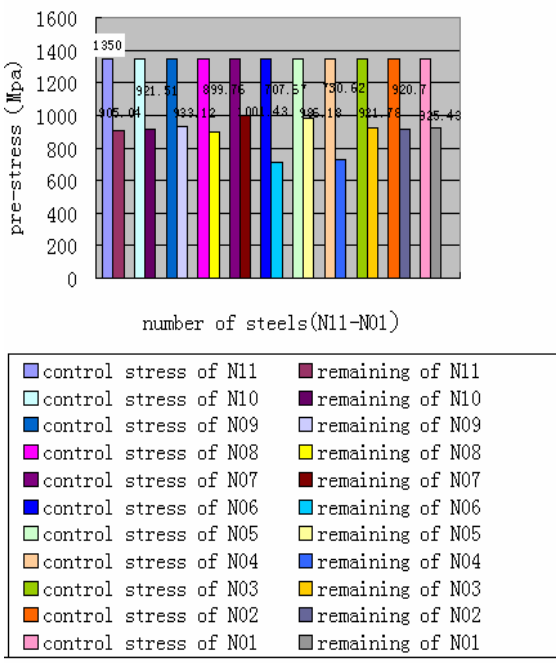


Fig.4. Comparison of remaining pre-stress and control stress

REFERENCES

[1] Zhang Jirao，*Cantilever Prestressed Continuous Beam Bridge*, China communiacations press, 2004.

[2] Xu Junlan, *Construction Control of Long-Span Bridges*, China communiacations press, 2000.

[3] Zhou Junsheng, Lou Zhuanghon, *Actuality and Development Tendency of Long-Span Prestressed Conninuous Bridges*, China journal of highway and trandport, January 2000, pp. 25-29.

[4] Ma Jianzhong, "Anidealized Nonlinear Backstep Analysis Method and Computer Simulation," *Shanxi Science and Technology of Communications*, August 2002, pp.46~48.

[5] Yu Kun, Tang Xiaobing, "Identifications of Damages in Bridges Structures Based on Combining Neural Network and Genetic Algorithm," *Journal of Wuhan University of Technology*, April 2006, pp.279-281.

[6] Masri S.F, Chassiakos A.G, Caughey T K, "Identification of Nonlinear Dynamic Systems Using Neural Networks," *Journal of Applied Mechanics*, NO.60, January 1993, pp.123~133.

[7] Chassiakos A.G, Masri S.F, "Modeling Unknown Structural Systems Through the Use of Neural Networks," *Earthquake Engineering and Structural Dynamics*, NO.25, February 1996, pp. 117-128.

[8] Liang Yanchun, Zhou Chunguang, Wang Zaishen, "Identification of Restoring Forces in Non-Linear Vibration Systems Based on Neural Networks," *Journal of Sound and Vibration*, NO.206, January 1997, pp.103~108.

[9] Liang Yanchun, Yang Xiaowei, Zhou Chunguang *et al*, *Application of Neural Networks to Identification of Nonlinear Characteristics in Cushioning Packaging*, Mechanics Research Communications, NO.23, June 1996, pp. 607-613.

[10] Liang Yanchun, Wang Zheng, Yang Xiaowei *et al*, *Identification of Non-Linearities in Cushioning Packaging Using Neural Networks with Fuzzy Adaptive Control*, Mechanics Research Communications,NO.24, April 1997, pp. 447-455.

Objective Evaluation of Seam Pucker Using SFC-RBFNN

Yonghui Pan [1,2] Fang Bao[1,2] ShiTong Wang[1]
[1]School of Information Technology, Southern Yangtze University
[1]No. 1800, Lihudadao, Wuxi Jiangsu 214122, China
[2]Jiangyin polytechnic college
Email: pyh.1972@yahoo.com.cn

ABSTRACT

In this paper, a supervised fuzzy clustering RBF neural network (SFC-RBFNN) is introduced for constructing the seam pucker evaluation system. Our experimental results demonstrate that the proposed system could efficiently be used as an objective seam pucker evaluation system with high accuracy and is robust for various structures and mechanical properties of middle-thickness woolen fabric.

Keywords: Seam Pucker Grade, Radial Basis Function Neural Network, Supervised Fuzzy Clustering, Principal Factor

1. INTRODUCTION

AATCC Method 88B-1992 has been commonly used for the subjective evaluation of seam pucker. According to this method, the appearance of seams are compared with photographic standards and the severity of seam pucker is graded into five classes, Class 5 being little or no pucker, and Class 1 severe pucker. Normally, Class 5 and 4 are acceptable, Class 3 is critical or borderline, and Class 2 and 1 are unacceptable. The merit of this method is directness, simple, low investment and easy to master, but it is influenced by uncertain factors of evaluating people and loses its objectivity easily.

Recently, many methods have been developed for objective evaluation of seam pucker. Among these methods, the relatively matured are listed as follows: J. Amirbayat uses strain of sewing thickness to evaluate seam pucker objectively [1]. A. M. Manich applies multi-regression to establish the sewing index prediction model for pure wool and blend fabric [2]. G. Stylios uses image processing technology to evaluate seam pucker of fabric quantitatively by extracting the sewing factors of fabric gray images [3]. C. K. Park employs three dimensional imaging analysis technology and artificial intelligence technology to evaluate seam pucker through five wrinkle shape parameters [4]. J. Fan proposes an objective evaluation system with tridimensional laser scanning technology to evaluate seam pucker [5].

Due to the sensitivity of small load area of fabric sewability, the spread, bending, sewing of small load area will cause the quality problem in the course of fabric spreading, cutting, sewing. Thus, mechanical properties of fabric under low stress are closely related to the production process of garments. By analyzing the correlation between the mechanical properties of middle thickness fabric which is measured by FAST (Fabric Assurance by Simple Testing) system and fabric sewability, we propose an objective evaluation method based on improved SFC-RBFNN (supervised fuzzy clustering RBF neural network).

The paper is organized as follows. Section 2 presents the individual steps of our approach for SFC-RBF neural network. Section 3 discusses the experiment results. In the final section conclusions are given.

2. SFC-RBF NEURAL NETWORK

2.1 RBF Neural Network

The topology of the RBFNN is shown in Fig. 1. Each hidden node evaluates a kernel function (receptive field) $\phi_i(\mathbf{x})$ on the incoming input, and the output $y(\mathbf{x})$ is simply a weighted linear summation of the output of the kernel functions [6,7]:

$$y(\mathbf{x}) = \sum_{i=0}^{c} w_i \phi_i(\mathbf{x}) \qquad (1)$$

In the case of the Gaussian basis functions, for example, we have

$$\phi_i(\mathbf{x}) = \exp(-\frac{\|\mathbf{x}-\mathbf{v}_i\|^2}{2\sigma^2}) \qquad (2)$$

Where $\mathbf{x}$ is the *n*–dimensional input vector, and $\mathbf{v}_i$ is the vector determining the center of basis function $\phi_i(\mathbf{x})$. Each kernel function gives its higher output when the input is closer to its center, and value decreases monotonically as the distance from the different forms, but the Euclidean distance is the most popular one, and is also used by us. The training phase of RBF neural network is accomplished in two separated steps: (1) training of the first layer weights (i.e. the kernel functions centers) by means of a clustering procedure and (2) calculation of the hidden to output weights by solving a system of linear equations.

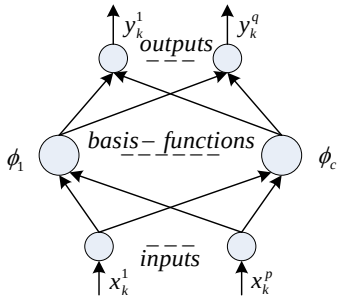


Fig.1. Topology of RBFNN

In our network, the RBF kernels do not assume any explicit functional form such as Gaussian, ellipsoidal, etc., but directly rely on the computation of the relevant distances. Let us suppose to have already determined the kernel function centers $\mathbf{v}_1, \cdots, \mathbf{v}_c$, the RBF units determine the level of matching of the current pattern $\mathbf{x} \in R^n$ with the given prototypes $\mathbf{v}_1, \cdots, \mathbf{v}_c$. Each of these prototypes is associated with its corresponding RBF unit. Let us denote the obtained levels of matching by $m_1, m_2, \cdots, m_c$. The matching level m_i is inversely proportional to the distance between $\mathbf{x}$ and the prototype of the *i*th RBF unit, $\mathbf{v}_i$. More specifically, the activation level m_i of the *i*th receptive field is based upon the similarity of $\mathbf{x}$ and the prototype of the field. Since these levels sum up to one (for proper normalization), this leads us to the optimization problem

$$\min_{m_1,\cdots,m_c}\left\{\sum_{i=1}^{c} m_i^2\left\|\mathbf{x}-\mathbf{v}_i\right\|^2\right\} \quad (3)$$

Subject to

$$\sum_{i=1}^{c} m_i = 1 \quad (4)$$

The use of the Lagrange multipliers method leads to the solution

$$m_i = \frac{1}{\sum_{j=1}^{c}\left(\frac{\left\|\mathbf{x}-\mathbf{v}_i\right\|^2}{\left\|\mathbf{x}-\mathbf{v}_j\right\|^2}\right)} = \phi_i(\mathbf{x}) \quad (5)$$

We shall see how to properly modify this expression in order to fully exploit the fuzziness involved in the procedure to determine the basis function centers; for now it is enough to say that the neuron situated in the output layer carries out a linear combination of the matching levels, yielding

$$y_k^i = \sum_{i=1}^{c} w_i m_i \quad (6)$$

Where $w_1, w_2, \cdots, w_c$ are the hidden-to-output weights. This expression can be formulated in a matrix notation as follows:

$$\mathbf{y}(\mathbf{x}) = WM \quad (7)$$

Where $W = (w_j)$ and $M = (M_i)$. We can optimize the weights by minimization of a suitable error function. It is particularly convenient to consider a sum-of-squares error function given by

$$E = \frac{1}{2}\sum_n \left|\mathbf{y}^n(\mathbf{x}) - \mathbf{t}^n\right|^2 \quad (8)$$

Where $\mathbf{t}$ is the target value for the output unit when the network is presented with input vector $\mathbf{x}$. Since the error function is a quadratic function of the weights, its minimum can be found in terms of the solution of a set of linear equations:

$$M^T M W^T = M^T T \quad (9)$$

Where $(T) = \mathbf{t}$ and $(M) = \phi(\mathbf{x})$. The formal solution to the weights is given by

$$W^T = M^P T \quad (10)$$

Where the notation M^P denotes the pseudo-inverse of M. Thus, the second layer weights can be found by fast, linear matrix inversion techniques.

2.2 Fuzzy C-Means Clustering

The Fuzzy c-means (FCM) clustering algorithm is a set-partitioning method based on Picard iteration through necessary conditions for optimizing a weighted sum of squared errors objective function (J_m). Let $c \geq 2$ be an integer; let $X = (\mathbf{x}_1, \cdots, \mathbf{x}_N) \subset R^n$ be a finite data set containing at least $c < N$ distinct points; and let R^{cN} denote the set of all real $c \times N$ matrices. A non-degenerate fuzzy c-partition of $\mathbf{x}$ is conveniently represented by a matrix $U = [u_{ik}] \in R^{cN}$, the entries of which satisfy [7]:

$$u_{ik} \in [0,1], 1 \leq i \leq c, 1 \leq k \leq N \quad (11)$$

$$0 < \sum_{k=1}^{N} u_{ik} < N, \quad 1 \leq i \leq c \quad (12)$$

The FCM algorithm was developed to minimize the objective function

$$J_m = \sum_{k=1}^{N}\sum_{i=1}^{c} (u_{ik})^m d(\mathbf{x}_k, \mathbf{v}_i), \quad 1 < m < \infty \quad (13)$$

In (13), $d(\mathbf{x}_k, \mathbf{v}_i)$ is any inner product norm metric of the distance between the feature vector $\mathbf{x}_k \in X$ and the prototype $\mathbf{v}_i \in R^n$. A metric often used in applications is the squared Euclidean distance between $\mathbf{x}_k$ and $\mathbf{v}_i$, that is $d(\mathbf{x}_k, \mathbf{v}_i) = \left\|\mathbf{x}_k - \mathbf{v}_i\right\|^2$. The coupled first order necessary conditions for solutions (U, V) to $\min\{J_m(U,V)\}$ are

$$u_{ik} = \frac{1}{\sum_{j=1}^{c}\left(\frac{\left\|\mathbf{x}_k - \mathbf{v}_i\right\|}{\left\|\mathbf{x}_k - \mathbf{v}_j\right\|}\right)^{(2/(m-1))}}, \quad \begin{matrix} 1 \leq i \leq c \\ 1 \leq k \leq N \end{matrix} \quad (14)$$

$$\mathbf{v}_i = \frac{\sum_{k=1}^{N} u_{ik}^m \mathbf{x}_k}{\sum_{k=1}^{N} u_{ik}^m}, \quad 1 \leq i \leq c \quad (15)$$

2.3. Supervised Fuzzy C-Means (SFCM) Clustering

In this section, we extend the original FCM objective function used by linear summation sub-networks and propose a supervised fuzzy c-means clustering (SFCM) model. Rather than defining J based on $\mathbf{x}_k \in R^n$ only, we supply it with information on the output space by defining a new objective function which assumes the following form:

$$J = \sum_{k=1}^{N}\sum_{i=1}^{c} (u_{ik})^m \left(\left\|\mathbf{x}_k - \mathbf{v}_i\right\|^2 + \left|\mathbf{y}_k - \mathbf{y}_k^*\right|^2\right) \quad (16)$$

where $\mathbf{y}_k$ and $\mathbf{y}_k^*$ are the corresponding desired output and computing output of sub-networks respectively. The first term of formula (16) denotes fuzzy c-partitions of input patterns $\mathbf{x}_k$ by minimizing the distance between inputs $\mathbf{x}_k$ and prototypes $\mathbf{v}_i$. The second term of formula (16) requests the computing output of system to approach the desired output mostly.

Now, by applying the Lagrange multipliers technique to (16), we derive the necessary conditions for the partition matrix and the prototypes, namely

$$u_{ik} = \frac{1}{\sum_{j=1}^{c}\left(\frac{\left\|\mathbf{x}_k - \mathbf{v}_i\right\|^2 + \left|\mathbf{y}_k - \mathbf{y}_k^*\right|^2}{\left\|\mathbf{x}_k - \mathbf{v}_j\right\|^2 + \left|\mathbf{y}_k - \mathbf{y}_k^*\right|^2}\right)^{1/m-1}}$$

$$1 \leq i \leq c, 1 \leq k \leq N \quad (17)$$

$$\mathbf{v}_i = \frac{\sum_{k=1}^{N} (u_{ik})^m \mathbf{x}_k}{\sum_{k=1}^{N} (u_{ik})^m}, \quad 1 \leq i \leq c \quad (18)$$

The structure of SFCM is shown in Fig. 2.

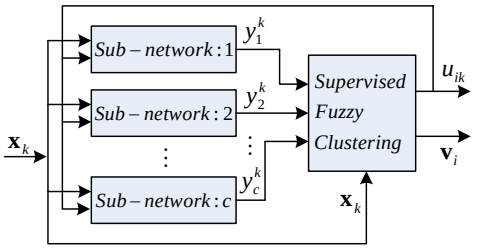


Fig.2. Construction of SFCM

There are two parts in SFCM model. One is supervised fuzzy classifier, and the other is linear summation sub-networks [8]. Let $\{\mathbf{x}_1, \cdots, \mathbf{x}_N\} \subset R^n$ be the patterns to cluster and $\mathbf{y}_k \in R^q$, $k = 1, \cdots, N$ be the corresponding desired output. Suppose to organize the data in *c* clusters, we can associate a local linear summation model for each cluster. The topology of the linear summation sub-network is shown in Fig. 3.

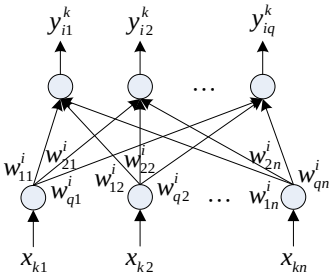


Fig.3. Topology of sub-network

Where $\mathbf{w}_i = (\mathbf{w}_1^i, \mathbf{w}_2^i, \cdots, \mathbf{w}_q^i)^T$, $\mathbf{w}_{ij} = (w_{j0}^i, w_{j1}^i, \cdots, w_{jn}^i)$, and the output of ith sub-network is $\mathbf{y}_k = \mathbf{w}_i \mathbf{x}_k$.

In order to calculate the weights of the ith sub-network $\mathbf{w}_i \in R^n$, $i = 1, \cdots, c$, we solve c least square problems, that is, one for each sub-network:

$$\min V = \frac{1}{2}\sum_{k=1}^{N} \{u_{ik}\mathbf{w}_i\mathbf{x}_k - \mathbf{y}_k\}^2 \qquad (19)$$

We can rewrite this expression in the form

$$\min V = \frac{1}{2}\sum_{k=1}^{N} \{\mathbf{w}_i\psi_i(\mathbf{x}_k) - \mathbf{y}_k\}^2 \qquad (20)$$

Where $\psi_i(\mathbf{x}_k) = u_{ik}\mathbf{x}_k$

Differentiating (20) with respect to the parameters $\mathbf{w}_i$ and setting the derivative to zero we obtain

$$\frac{\partial V}{\partial \mathbf{w}_i} = \sum \{\mathbf{w}_j\psi_j(\mathbf{x}_k) - \mathbf{y}_k\}\psi_i(\mathbf{x}_k) = 0$$

$$j = 1, \cdots, c \qquad (21)$$

Writing (21) in matrix notation we have $(\psi^T\psi)W^T = \psi^T Y$, and then

$$W^T = \psi^P Y \qquad (22)$$

Where ψ^P denote the pseudo-inverse of matrices ψ.

2.4. The Algorithm for SFCM Clustering

The algorithm is composed of the following steps (see Fig. 4). At the end of the clustering process, the set of prototypes obtained by the algorithm is used in the RBFNN architecture previously described, and then the pseudo-inverse approach is performed to optimize the hidden to output weights. When the system is presented with a new input pattern $\mathbf{x}$, the RBFNN computes the activation level ϕ_i, $i = 1, \cdots, c$, through the expression (5) suitably modified and then these values are combined together to compute the RBFNN output using (6).

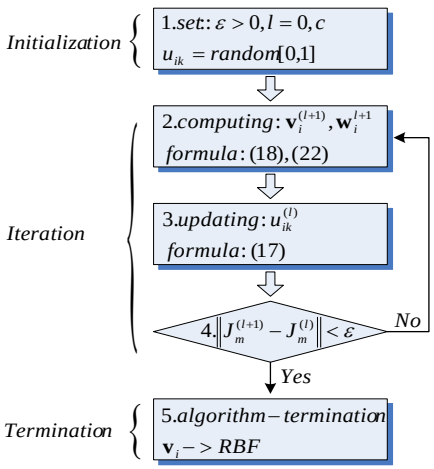


Fig.4. Steps of SFCM algorithm

3. EXPERIMENTAL RESULTS

In this paper, we apply FAST (Fabric Assurance by Simple Testing) system to test the low stress mechanical properties of middle-thickness woolen fabric. The FAST system is simple to operate to predict the formability, machinability of fabric, dimensional stability of garment with the use of fingerprint chart. And the prediction can give constructive suggestions and

manufacture instructions to garment manufacturer and fabric factory respectively. We choose 36 pieces of middle-thickness woolen fabric as test samples. The basic specifications of the test samples are shown in table 1.

Table 1. Basic parameters of test samples

sample	ends per inch	picks per inch	fabric weave	fabric weight (g/m^2)	fabric thickness (mm)
middle -thickness wool fabric	53.8-94	42.2-71.6	plain; twill; satin	141-250	0.320-1.103

The test samples are 30cm×60cm sewing threads. Both the above and nether sewing threads have been sewed in the middle along the same fabric grain direction. Because the direction of fabric cutting piece must be always the same in most cases, we only consider the seam pucker grade when the direction of both the above and nether cutting piece is the same. In this paper, we pay more attention to the influence of mechanical properties on the sewability of middle-thickness woolen fabric but not to the influence of sewing conditions. According to the practical manufacture experience, we impose corresponding sewing conditions to make the different sewing threads. The sewing samples have been sewed by skilled workers using suitable flat sewing machine. The sewing conditions are shown in the Table 2. The sewing threads which have been washed and aired well are evaluated with AATCC-88B criterion to get corresponding seam pucker grade by two experts.

Table 2. Specification of needle and thread

needle size (unit style)	thread type (tex)	stitch length (3cm)
14	13.9×3	11-14

Evaluating the sewability along five different directions, we measure and compute the corresponding mechanical properties of each fabric, and get 180 of groups experiment data. Thereinto, 144 groups of data are used to training neural network, and the rest 36 groups are used to simulate. According to Pearson rank-order correlation method, we find great correlation among these mechanical properties. So we remove those properties which are highly correlated with each other and those scarcely related to fabric sewability, and apply main factor method to analyze the reserved factors to get rid of the redundant information [9]. At last, we get six simple and effective main factors as the input of the RBF neural network. And the seam pucker grade of AATCC-88B is as the output of neural network. The definitions of six main factors are shown in Table 3.

Table 3. Definitions of main factors

main factor		relative index
1	moldability	warp bending rigidity; weft bending rigidity; 45 º diagonal bending rigidity; warp formability; weft formability
2	heavy	fabric thickness under 2gf; fabric thickness under 100gf; fabric surface thickness; fabric weight (g/m^2)
3	warp action	warp tensile strength under 5gf/cm; warp tensile strength under 20gf/cm; shearing rigidity
4	45º diagonal action	diagonal tensile strength under 5gf/cm; diagonal tensile strength under 20gf/cm; weft formability
5	weft action	weft tensile strength under 5gf/cm; weft tensile strength under 20gf/cm
6	dimensional stability	warp relaxation shrinkage; weft relaxation shrinkage

The above mentioned six main factors are orthogonal and independent. According to weight coefficients of the original variable in main factors, we can obtain corresponding dimensionless computing value of each main factor.

Due to the number of the main factors and the seam pucker grade of subjective evaluation has been fixed, we set the corresponding node number of the input layer, hidden layer, and output layer of network is 6, 12 and 1 respectively, and let the weight coefficient of SFCM clustering M=2. Reference [10] uses ordinary BP neural network to evaluate seam pucker, and sets the number of hidden layer equal to 6 and the objective error equal to 0.1. The optimizing iteration number of BP network is about 35000. In this paper, we apply improved SFC-RBF neural network to evaluate seam pucker. By large numbers of testing, we find the convergence speed of our algorithm is very fast on the same objective error 0.1, and the iteration number of SFCM is about 10^3 degree. The 36 groups of testing data in table 4 is the prediction results of seam pucker grade which are evaluated by ordinary BP network (reference [10]) and improved SFC-RBF network respectively.

Table 4. Predicted of BP network and SFC-RBF network

samples	subjective evaluation	ordinary BP network		SFC-RBF network	
		objective evaluation	relative error	objective evaluation	relative error
1#	5.00	5.1	2.00%	4.96	1.20%
2#	4.00	4.32	8.00%	4.15	3.75%
3#	5.00	4.87	-2.60%	5.06	1.20%
4#	3.00	3.19	6.33%	3.04	1.33%
5#	5.00	4.93	-1.40%	4.97	-0.60%
6#	4.00	3.92	-2.00%	3.86	-3.50%
7#	3.50	3.79	8.29%	3.39	-3.14%
8#	5.00	4.66	-6.80%	4.97	-0.60%
9#	4.50	4.85	7.78%	4.41	-2.00%
10#	4.50	4.46	-0.89%	4.46	-0.89%
11#	3.50	3.1	-11.4%	3.49	-0.29%
12#	4.50	4.33	-3.78%	4.55	1.11%
13#	4.00	4.4	10.00%	3.74	-6.50%
14#	4.00	3.88	-3.00%	3.87	-3.25%
15#	4.00	4.31	7.75%	4.33	8.25%
16#	4.50	4.75	5.56%	4.44	-1.33%
17#	5.00	4.94	-1.20%	4.88	-2.40%
18#	4.50	4.68	4.00%	4.15	3.75%
19#	5.00	5.25	5.00%	4.34	-3.56%
20#	5.00	4.68	-6.40%	4.92	-1.60%
21#	4.00	3.93	-1.75%	4.89	-2.20%
22#	4.00	3.85	-3.75	3.91	-2.25%
23#	4.50	4.06	-9.78%	4.23	5.75%
24#	4.50	4.64	3.11%	4.52	0.44%
25#	4.50	4.61	2.44%	4.69	4.22%
26#	4.50	4.40	-2.22%	4.44	-1.33%
27#	5.00	4.68	-6.40%	4.43	-1.56%
28#	4.00	3.97	-0.75%	5.16	3.20%
29#	4.00	3.90	-2.50%	3.89	-2.75%
30#	4.00	3.72	-7.00%	3.88	-3.00%
31#	3.50	3.57	2.00%	4.12	3.00%
32#	4.00	3.89	-2.75%	3.41	-2.57%
33#	4.50	4.23	-6.00%	3.89	-2.75%
34#	5.00	4.56	-8.80%	4.39	-2.44%
35#	3.00	2.92	-2.67%	4.87	-2.60%
36#	3.00	3.25	8.33%	3.12	4.00%

From table 4, we can see the prediction results of SFC-RBFNN is more closer to the subjective evaluation values, the biggest relative error is below 8.5%, and the whole prediction accuracy is much better. To quantitatively describe the relativity between the objective evaluation and subjective evaluation, we compute the relative coefficients of the ordinary BP network and SFC-RBF network respectively through the results of table 4. The relative coefficients are shown in Fig.5.

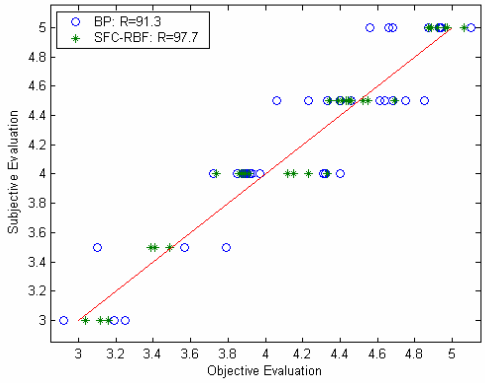


Fig.5. Relative coefficients of BP and SFC-RBF network

From Fig. 5, we also can see both two methods have higher relative coefficient. The correlation coefficients of the ordinary BP network and SFC-RBF network are 91.3% and 97.7% respectively, but the SFC-RBF network have much better prediction capability.

4. CONCLUSIONS

In this paper, we propose an objective seam pucker grade evaluation system based on improved supervised fuzzy clustering and RBF neural network. This system can evaluate the seam appearance grade of fabric fast, effectively and objectively. But with the limitation of our time and energy, the system we proposed still has some deficiencies: The first is the number of fabric samples we used is not abundant. Because the kinds and the structures of woolen fabric are very complicated and various, we can not choose all kinds of fabric as our samples, but some middle-thickness woolen fabric which is often used and has ordinary structure. The system we established only can predict the same or approximate kind of

fabric. So how to improve the generalization capability of this objective evaluation system is the important aspect in the future. The second is that more and more manufacturers and traders of woolen fabric want to get helpful suggestions from the fabric sewability prediction software as FAST system becomes more popular. If we can develop corresponding software with kindness interface and powerful database support, our objective evaluation system will be more wildly applied. Things mentioned above will be researched further in the future.

REFERENCES

[1] J. Amirbayat, "Seams of different ply properties, Part 1:Seam Appearance, Part 2:Seam Strength", *Journal of the Textile Institute*, Vol.82, No.2, 1992, pp.211.

[2] A. M. Manich, J. P. Domingues et al, "Relationships between fabric sewability and structural, physical, and FAST properties of woven wool and wool-blend fabrics", *Journal of the Textile Institute*, Vol.89, No.3, 1998, pp.579~591.

[3] G. Stylios, J. Sotomio, "A Neural network approach for the optimization of the sewing process of wool and wool mixture fabrics", Proc. of 1st China International Wool Textile Conference, Xi'an, 1994, pp.689~693.

[4] K. P. Chang, J. K. Tae, "Objective rating of seam pucker using neural networks", *Textile Research Journal*, Vol.67, No.7, 1997, pp.494~502.

[5] J. Fan, F. Liu, "Objective evaluation of garment seams using 3Dlaser scanning Technology", *Textile Research Journal*, Vol.70, No.6, 2000, pp.1025~1030.

[6] B. Ye, C. Z. Zhu et al, "Adaptive extended fuzzy basis function network", *Neural Computing & Applications*, Vol.16, 2007, pp.197~206

[7] K. B. Kim, J. H. Cho et al, "Recognition of Passports Using FCM-Based RBF Network", *Australian Joint Conference on Artificial Intelligence*, 2005, pp.1241~1245.

[8] Y. H. Liu, Q. Liu et al, "Speech Recognition Based on Fuzzy Clustering Neural Network", *Chinese Journal of Computers*, Vol.29, No.10, 2006, pp.1894~1900

[9] Y. L. Hu, S. H. He, Synthetical evaluation method, Beijing: Scientific Inc. Pub., 2000.

[10] K. Liu, Objective evaluation systems of the garment seam pucker grade based on mechanical properties of fabric. Shanghai: Donghua University, 2005.

Yonghui Pan is PhD candidate of School of Information Technology, Southern Yangtze University and vice president of Jiangyin Polytechnic College. His research interests are in fuzzy system and swarm intelligence.

Predicting Clinker Strength Based on Matlab Neural Network *

Lifang Chen [1,2] Liang Chen [3] Rulin Wang [1]
[1]School of Mechanical Electronic & Information Engineering,
China University of Mining & Technology BeiJing, China
[2]College of Science, Hebei Polytechnic University,
Tangshan, Hebei, China, 063009
[3]Information Engineering Department,
Tangshan Institute of Vocation and Technology, Tangshan, Hebei ,China,063004
Email: chenlifang@heut.edu.cn

ABSTRACT

The paper presents principles of BP network and emulation method by MATLAB on the premise of studying predict method of clinker strength. The authors designs training program and verify it by an actual example. From the result, it can be seen that after training the network has better prediction ability and proves to be of practical value in predicting clinker strength. Applying our model via neural network package in MATLAB to guide the cement production and to determine the admixture further is very important. Meanwhile, it provides the theoretical evidence for ensuring the quality of cement.

Keywords: Neural Network, BP Algorithm, Admixture, Clinker Strength

1. INTRODUCTION

A new standard has been applied to Chinese cement field on April 1, 2001. In order to obtain high quality cement product, excellent clinker is necessary. The strength of cement is related to many factors, among which the most important is clinker strength. Predicting clinker strength is a multivariable, non-linear, long-time problem. In the process of cement production, one of the main bases of measuring cement strength is the 28th-day strength value. Although the 28th-day strength value and its influential factors whose physical and chemical performance are detectable, the quantitative relationship between detection values and cement strength cannot be formulated by a function.[1]

According to the new standard, the relationship between the 28th-day strength value and mineral components has been changed. Finding the relationship will be helpful for guiding cement production. By investigating the relationship between the mineral components of clinker and the clinker strength, we can predict the clinker strength effectively. [2] According to the specific scenarios of the cement factories, we can determine the filling of admixture to control the cement strength declination and thus to predict the cement production effectively.

Traditional linear regression prediction methods, which treat the nonlinear relationship between cement strength and other measure values as linear ones, cannot produce the correct result.[3,4] We cannot use clustering prediction fixed method, which immobilize the cement strength values as some cluster middle values, on the nonlinear problem like cement strength since it lacks the genetic ability. Neural network based on physiology seeks out principles by studying samples, summarizing and rearranging.[10] The appearance of neural network provides an effective tool for establishing complex nonlinear function model .[11] In this paper, we use neural network, which can approach any nonlinear function indefinitely, to create the cement clinker strength model. MATLAB can be used to implement the cement clinker model.

2. BP ALGORITHM & MATLAB

2.1 BP Algorithm

Back-propagation algorithm is a kind of supervised learning algorithm. The learning process of BP algorithm consists of two phases. The first phase is called forward-propagation. In this phase, inputted from the input layer and after being processed by the hidden layer, the information then propagated to the output layer. Only the state of neurons in the previous layer can affect that of the next layer. If the output doesn't meet the expectation in the output layer, the learning process would go into the second phase, back-propagates, and the network adjusts the weights of each neuron passing it. The structure of network is depicted in fig.1.

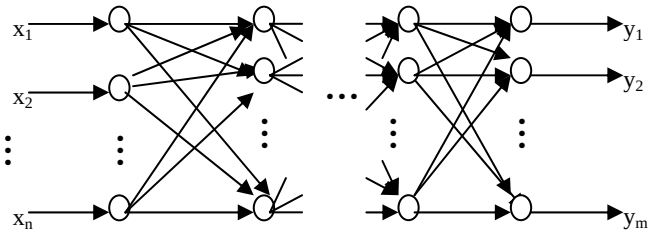


Fig.1. Structure of BP network

2.2 MATLAB Neural Network

Designed by Mathworks Company MATLAB is a software product used in education, engineering and science calculation. It provides a perfect integrated environment which includes concept design, algorithm development, construct model, emulation and real time realization. MATLAB is an effective tool in scientific research, product development and education area.

The neural network toolbox (NN toolbox) of MATLAB is the prime choice for engineers to design and analyze neural network. NN toolbox, based on neural network and using MATLAB, constructs many typical activate function, such as S function, linear function, compete function and so on. By doing so, designers can change their output calculation into calling activate function, simplifying their calculation. In addition, the users can add training process of network according to different typical ameliorate regulars and compile training programs by MATLAB. The designer of

* Hebei Province Bureau of Science & Technology, Project No: 042135130

networks can focus their energy on thinking about problems, so as to improve efficiency and quality in solving problems [12].

3. CONSTRUCTING PREDICT MODEL & TRAINING

3.1 Analysis on Factors Influencing Clinker Strength

Clinker strength predication is a multivariable and non-linearity problem. [5] In the process of cement production, there are many factors to affect clinker strength in which the most important is chemical ingredient, mineral constitution and structure of mineral rock facies. The main mineral constitutions of silicate clinker include C_3S, C_2S, C_3A, C_4AF, SO_3, f—CaO, MgO, R_2O. Next we will analyze the contribution of the composition to clinker strength.

1) C_3S, C_2S, C_3A, C_4AF: Their hydrate leads to cement's jelling. Accordingly, the contents of C_3S, C_2S, C_3A, C_4AF play the most important role to clinker strength.
2) SO_3: In order to keep pace with production, adjust SO_3 after grating between 2.3 ± 0.1 by adding natural two H_2O gypsum in grate. Therefore, SO_3 is not considering as an input parameter in prediction.
3) f-CaO: In the temperature of reaction sintering, the structure of free lime is compact, it reacts relatively slowly with water. Generally speaking, the reaction is obvious after adding water 3 days later. When free lime reacts with water into $Ca(OH)_2$, the volume expands by 97.9%, building up part swelling stress inside harden cement. Since free lime increases in cement, tensile strength and flexural strength decrease, and then after 3 days the strength will retrogress, seriously conducing unsteadiness, leading to the production of cement distort or cracking and destroying the cement paste. Therefore, the content of free lime should be controlled strictly. In this paper, f-CaO is considered as an input parameter in predicting.[6,9]
4) MgO: Because MgO reacts with water more slowly than free lime, it will be obvious after months and years. When MgO reacts with water into $Mg(OH)_2$, the volume expands by 148%, also leading to unsteadiness.[7,8] The content of MgO must be controlled strictly. Because it has no effect on early phase of cement hydrate, in this paper, MgO is not considered as a parameter.
5) R_2O: The alkali of clinker will make alite and tricalcium aluminate react more quickly with water, so the strength of cement with alkali will be improved in the early phrase. After or at 28^{th}-day, the strength will decrease. In this paper, R_2O is considered as an input parameter.

In the research, six parameters (C_3S, C_2S, C_3A, C_4AF, f—CaO, R_2O) were selected.

3.2 Construct of Predicted Model

Through the following work we find the optimal training parameters of BP. These parameters include the number of hidden nodes, the learning rate and the transfer function between hidden neurons and output neurons, which play an important role in the performance of the net. The input nodes are determined by the problem to be solved and the data expression mode in designing BP network. According to analysis about affecting factors of clinker strength, six parameters were selected (C_3S, C_2S, C_3A, C_4AF, f—CaO, R_2O) to be input layer's nodes and two parameters as output layer's nodes. The hidden layer nodes need to be selected by emulation. By a lot of experiment, the result showed 15 is optimal. We choose 6-15-2 BP network. The structure of prediction model is depicted in fig.2.

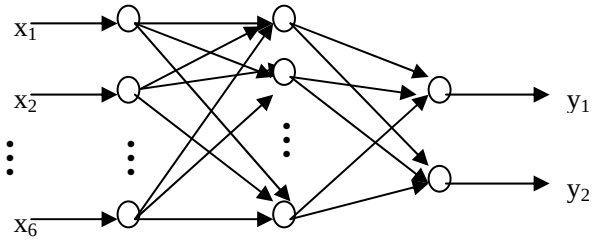


Fig.2. Predicting model

3.3 Network Training

The network will be used to predict clinker strength in production after training. Because of the complex structure of network and the great number of nodes, the learning rate is 0.1.

Tabel 1 Training parameters

Training numbers	Training target	Learning rate
1000	0．001	0．1

The codes are as follows:

```
clear all;
P=[·····]';
T=[·····]';
P_test=[·····]';
T_test=[·····]';
threshold=[- 1 1;-1 1;-1 1;-1 1;-1 1;-1 1];
net=newff(threshold,[15,2],{'tansig','purelin'},'traingdx');
net.trainParam.epochs=1000;
net.trainParam.goal=0.001;
LP.lr=0.1;
net=init(net);
net=train(net,P,T);
temp=sim(net,P);
y_out(1,:)=temp(1,:);
y_out(2,:)=temp(2,:);
temp=sim(net,P_test);
y(1,:)=temp(1,:);
y(2,:)=temp(2,:);
Y1=[y(1,:),y(2,:)];
Y2=[y_out(1,:),y_out(2,:)];
for i=1:10
    error1(i)=norm(Y1(:,i)-T_test(:,i));
end
figure;
plot(1:10,error1,'r');
hold off;
```

The network needs to be tested after training, so as to be applied into production.

4. APPLICATION

The following table 2 is data from JiDong cement Company which would be used as training and testing samples on prediction model.

Tabel 2 Data from JiDong cement Company

No	R_2O	fCaO	C_3S	C_2S	C_3A	C_4AF	3^{th}-day	28^{th}-day
1	0.78	0.5275	52.00	25.43	6.96	11.39	29.40	62.90
2	0.80	0.5326	55.54	21.62	7.15	11.31	29.60	63.80
3	0.85	0.6001	55.01	22.24	7.18	10.98	33.60	61.50
4	0.85	0.6717	57.03	20.49	6.57	11.05	34.10	61.40
5	0.89	0.6892	56.06	21.26	6.64	11.17	31.50	60.80
6	0.85	0.6479	56.73	20.48	6.75	11.26	33.00	63.00
7	0.89	0.595	49.53	27.43	7.25	10.93	30.00	63.70
8	0.87	0.7175	54.21	23.10	6.76	10.93	33.00	61.90
9	0.85	0.6908	57.21	19.70	6.70	11.61	34.50	58.80
10	0.86	0.675	59.65	17.43	6.52	11.45	35.00	58.80
11	0.87	0.6204	52.86	23.68	6.98	11.33	30.80	59.60
12	0.81	0.5542	51.28	25.64	6.77	11.48	30.00	60.90
13	0.88	0.5921	55.06	22.08	6.65	11.29	33.70	62.40
14	0.87	0.6767	55.53	21.56	6.82	11.35	34.30	61.30
15	0.87	0.5988	57.62	19.41	6.75	11.29	33.60	60.10
16	0.85	0.6309	56.15	20.72	6.82	11.41	31.40	60.30
17	0.85	0.6334	57.06	19.86	6.64	11.48	32.20	57.10
18	0.84	0.6879	56.09	21.05	6.63	11.38	32.40	60.20
19	0.84	0.6392	55.28	21.97	6.63	11.38	32.90	60.80
20	0.89	1.0261	53.58	23.47	6.41	11.57	33.20	61.10
21	0.81	0.665	56.48	20.40	6.38	11.62	30.80	59.50
22	0.78	0.6213	57.92	18.98	6.54	11.45	31.90	59.60
23	0.79	0.5446	48.88	27.42	7.05	11.51	28.50	61.00
24	0.83	0.5746	49.03	28.18	6.55	11.26	27.90	61.10
25	0.84	0.5088	51.41	25.20	7.01	11.33	29.30	62.20
26	0.85	0.6092	54.42	22.14	6.97	11.27	31.10	59.10
27	0.90	0.6113	55.34	21.22	6.79	11.27	32.30	58.50
28	0.90	0.6804	58.97	17.83	7.01	11.15	33.40	57.10
29	0.87	0.6134	57.19	20.08	6.65	11.05	31.10	58.50
30	0.87	0.7002	56.56	20.21	6.92	11.09	30.90	59.30

In the process of emulation, the first 20 group data are training samples. The last 10 groups are testing samples. Before training, the data must be normalized between-1 and 1. The difference curve of training and testing is depicted in fig.3.

Tabel 3 Result of network prediction

No	3^{th}-day-real	28^{th}-day-real	3^{th}-day-prediction	28^{th}-day-prediction	3^{th}-day relative diffrence	28^{th}-day relative difference
21	30.80	59.50	30.818534	59.4035155	0.06%	-0.16%
22	31.90	59.60	31.153159	59.1464145	-2.34%	-0.76%
23	28.50	61.00	27.389627	60.2123261	-3.90%	-1.29%
24	27.90	61.10	27.311239	58.5689321	-2.11%	-4.14%
25	29.30	62.20	29.288833	59.0271879	-0.04%	-5.10%
26	31.10	59.10	31.342248	58.4038615	0.78%	-1.18%
27	32.30	58.50	31.735615	57.8075327	-1.75%	-1.18%
28	33.40	57.10	33.527916	58.1396492	0.38%	1.82%
29	31.10	58.50	31.972928	58.247139	2.81%	-0.43%
30	30.90	59.30	32.32216	58.183961	4.60%	-1.88%

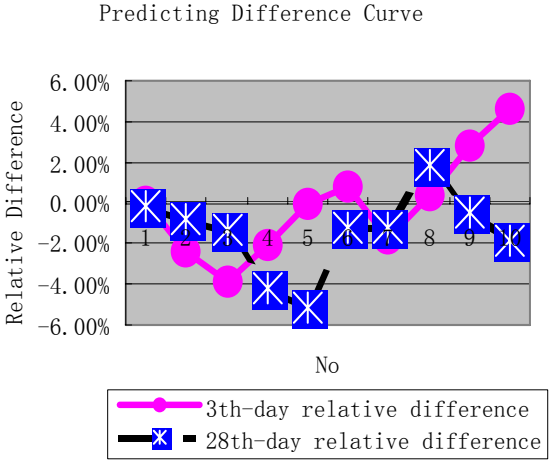


Fig.3. Predicting difference curve

It can be seen from Tabel 3 & figure 3 that the prediction deviation is very small which proved the network is reliable. The model can be used in production process to predict clinker strength of 3^{th}-day and 28^{th}-day. On the basis of the predicting result we can ascertain the filling amount of admixture.

5. CONCLUSIONS

Neural network package in MATLAB provides a lot of functions and commands which can be called directly. Developing project using MATLAB, which include neural network design and training, could solve problems effectively. Applying our model via neural network package in MATLAB to guide the cement production and the amout of admixture is very important. Meanwhile, it provides the theoretical evidence for ensuring the quality of cement.

REFERENCES

[1] Shin lchiro Hashimoto et al. “A Fundamental Study on Concrete Substituted Cement with Industrial By-Products.” *International Journal of Modern Physics B.* Volume 17, numbers 8-9/April 10, 2003.

[2] L.-L.Wang,S-Q.Shi,J-Y.Chen, et al. “Influences of Strain-Rate and Stress-State on Dynamic Response of Cement Mortar.” *International Journal of Structural Stability and Dynamics.* Volume 3, Number 3/ Sep. 2003.

[3] M.H.Simatupang, “Addition of metakaoline to Portland Cement, Influence on Hydration and Properties of Cement-bonded Wood Composites.” Holz als Roh und Werkstoff, Volume 56, Number 3, 2003.

[4] YiMinWei, etal. “Hydration behavior and Compressive Strength of Cement mixed with exploded wood fiber Strand Obtain by the Water-Vapor explosion Process.” *Journal of Wood Science*, Volume 49, Number 4, 2003.
[5] Francisco Moreno-Seco et al, “Extending Fast Nearest Neighbour Search Algorithms for Approximate K-NN Classification.” *Lecture Notes in Computer Science*, Volume 2652/2003.
[6] Yunhui Liu,etal, “Information Geometry on Modular and Hierarchical Neural Network.” *Lecture Notes in Computer Science*, Volume 2834/2003.
[7] Seree Supharatid, “Tidal-Level Forecasting and Filtering by Neural Network Model.” *Coastal Engineering Journal*, Volume 45, Number 1/March 2003.
[8] Yu ShiLian et al. “cement intensity forecast Based on the neural network,” *Hefei Industrial University Journal* (Natural Science) February 2002.
[9] WU You-fu et al. “A New Discern Algorithm of Mode Attribute Clustering & Application in Predicting Cement Strength,” *System Engineering Theory & Practice*, Jul 2002.
[10] BAI Shu-fang et al. “Adjust Mixture Plan & Improve ISO Clinker Strength based on Regression Analysis,” *YunNan Building Material*, Apr,2001.
[11] WEI Hai-kun, *The Theory & Method of Neural NetworkStructure Design*,” National Defence Industry Press.
[12] WEN Xin et al. *MATLAB Neural Network Application Design*, Science Press.
[13] LIU Wei-guo et al. *MATLAB Programming Design &Application*, Higher Education Press.

Lifang Chen: Female, 1973, Yutian Hebei, Associate Professor, Master, Research direction: Control theory and Control Engineering.

Evaluation of Argumentative Essays Based on BP Network

Wei Weng, Deiwei Peng
Wuhan University of Technology School of computer science and technology
Wuhan, hubei, China
Email: i.gavin.weng@gmail.com, pengdewei@whut.edu.cn

ABSTRACT

This paper describes the using of BP networks for evaluating human essays. Certain important features of an essay can be quantified and served as input as BP networks for scoring the essay. An experiment of using 80 essays as sample was conducted, and a comparison, based on 40 essays, between the score given by this method and the score by human scorers were made.

Keywords: Neural Network, BP Network, Essays Evoluation

1. INTRODUCTION

Unlike evaluations given by human readers, those given by computers are always highly reliable, since machines are not subject to any of the traits or conditions, such as impatience or fatigue, that make human evaluators less than perfectly consistent over the time[6]. Moreover, it reduces the impact of human's personal preferences on the evaluation. Program will generate the same result regardless of the differences between the computers that it is running in, so all the essays can be judged under the same stander [9].

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques [10]. A trained neural network can be thought of as an "expert" in the category of information that has been given to analyze [8]. Thus, using ANN is a good approach to score an essay based on raw sores for the relation between the four parts of raw scores and the final overall score of the essay is complex.

2. OBTAINING OF RAW SCORES

To obtain raw scores is to extract information, which is related to the quality of the essay, from the text. We divided the raw scores into four parts: The first one is named as vocabulary, and it is used to evaluate the using of English vocabulary in the essay; the second one is named as Sentence Skills, and it is used to score the sentence structure of the essay; the third one is cohesion, and it is for judging how the essay is organized and developed; the last one is content, which is to evaluate the materials and ideas contained in the essay [2].

2.1 Vocabulary

Generally speaking, the more syllables a word contains, the more advanced that word is. Taken those words that have the meaning of big as example, "titanic" is more advanced than "large" and "large" is more advanced than "big". To simplify this model, we use the number of the letters contained in a word instead. By scanning the text, the following date is acquired. Q stands for the average number of letters the words in the essay have. K is the number of words that have contained 6 to 9 letters, and X is those with 9 to 12 letters. Y is the number of words whose number of letters is larger than 12. Considering different amount have different weight, we use the following formula to get score:

A=q+ (k*5+x*20+y*40)/N; (N is the number of total words an essay contains)

Another aspect we have taken into consideration is the unnecessary repetition of using the same word [7]. As we know, many different English words can express the same meaning. For instance, "like", "fancy","love","prefer" and etc. share a common basic meaning although they have subtle differences. And if one person only uses one of them repeatedly, a lower score will be given in the word section. Some common words, such as "which", "that", "I", "you" and so forth, are not listed among the words that should not be repeated. Nouns are not in that list either. R is the occurrences of repetition we have found, so the final word score is given: F=A-R*3/N.

2.2 Sentence Skills

In measuring the author's ability to write English sentences, Firstly, it is the complexity o three aspects are taken into account.

f the sentence structure. A complete English sentence consists of many clauses, which are separated by some punctuation (",") is the most widely used one). P is the number of clauses the essay have, and Q is the number of complete sentence the essay have, so P/Q is the dater we use to measure the complexity of an essay's sentence structure.

Secondly, it is the variability of sentence structural. The changing of sentence not only demonstrates the writer's ability to use the language but also give readers intense atheistic feelings. Here, we use standard deviation of the number of words that the essay's complete sentence possesses to represent variability.

Thirdly, it is the parallel structure the essay has [5]. Parallel sentences read more smoothly than the nonparallel ones and they have conspicuous features. Consecutive sentences that form parallel structure share similar usage of English vocabulary or sentence structural. One example is Martin Luther king's famous speech" I have a dream", parallel structures are formed through sentences beginning with the same phrase" I have a dream". By comparing these features of sentences that are near in position, we can identify parallel structure.

At last, by combining those 3 aspects, we can score an essay's sentence skills:

S=A/2+D/9+P (A is the average number of clauses; D is the standard deviation; P is the number of parallel structural we identify and P has an upper limit of 3).

2.3 Cohesion

Many transitional words play an important role in the development and organization of English essay by making essays more cohesive [3, 4]. They are often used in connecting

the following parts of essay writing: stating thesis, showing author's position, listing main points, giving supporting materials, making conclusions and so forth. Hardly can any one find a well developed essay without those cue words.

We have made a list of roughly over 100 transitional words. Another problem is how to check the context and find out whether they really serve the function of connecting meanings. Take" at last" for example, if it occurs in the sentence" we win the game at last", it can not be counted as transitional words. And if it appears at the beginning of sentence and followed by a comma, it is highly possible that it serves as transitional word. For example" at last, I would like to say……..." .So through finding cue words and checking the context (especially their position in sentence and paragraph), we can identify cue words. P is the number of cue words that we have identified, Q is the number of sentences that the essay contains, so P*20/Q is the final score of cohesion.

2.4 Content

When we are talking about whether an essay has contained sufficient materials, we often consider the following aspects: 1, whether the given topic has been well analyzed. In other words, how many main points the author gives about that topic. 2, how well those points are supported. 3, whether the author state opinions and make conclusions.

A good essay has many paragraphs, and one paragraph is often related to one main idea. Usually, the first paragraph often provides introduction materials and shows author's position on a certain issue. The following ones are called main body, and each of them has its own main idea and supporting details. The last paragraph is used to make a conclusion.

By checking an essay's paragraphs, we can score its content. One thing we need to check is whether the essay is complete, checking whether it has beginning and conclusions and how many supporting ideas are presented. Another thing to check is how each separate paragraph is written. The last thing is the proportion of each paragraph. Introduction materials should not be too long and main body should not be too short. Through searching cue words in each paragraph and comparing the lengths of paragraphs, the things we have stated above can be done.

In sum, the four raw scores we obtained from the essay can reflect its quality to some extent and they will serve as input of BP networks.

3. EXPERIMENT

Different examinations have different scoring standers, but all of them aim at making distinguishes between those essays according to its quality by the means of giving them different scores. To maintain the consistency of scoring standerd, we have chosen one type of examination, the ISSUE writing of GRE's analytical writing test, to conduct our experiment. We have trained the BP networks with officially scored sample essays, and then we have made a comparison between the score given by human and score given by computer.

After several tries, this is how we design the BP network [1]:There are 3 layers in total in network. 4 knots in the input layer, 14 in the hidden layer and 1 in the output layer. We have set a goal of 0.05 of training, the graph below shows that the training process goes on well:

After the network is trained, we use it to score another 40 essays and compare the result to scores given by human reader. The result is showed as follows:

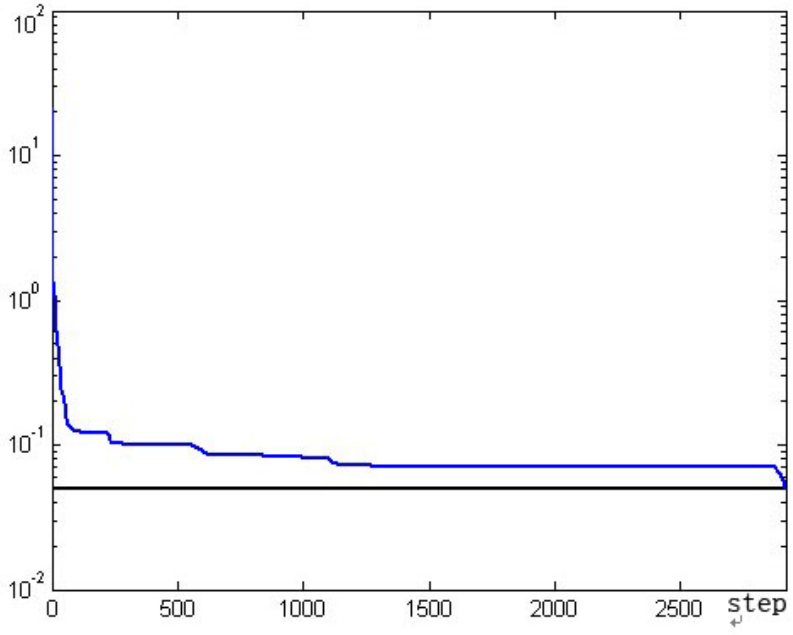


Fig.1. The Training Process of BP networks

Table 1 The result to scores given by human reader

Human given score	Computer given score						
1	7.3355	1.2718	-0.2369	0.9154	1.1637	1.0385	
2	1.7791	3.9164	2.0231	1.9281	0.8757	3.1	2.2653
3	2.7	3.8493	2.8167	3.2146	3.0572	2.9378	4.0258
4	5.1799	5.1376	4.2619	3.8495	4.1537	5.5984	
5	5.1	4.8658	5.0581	4.9923	4.7891	5.2499	6.2157
6	4.3076	5.7902	6.2463	7.5881	6.3542	5.9487	5.8256

4. DISCUSSION &CONCLUSIONS

Fig.1 shows the training process of neural networks. The line on that graph means the training target. For each point on the curve, the X-coordinate value is the training steps, and the Y-coordinate value is the gap between the output of network and the actual result of the sample. From the figure, we can see that the target has been reached within 3000 steps. This speed demonstrates that the network is appropriately designed.

The aim of computer score is to classify essays according to its quality. Human scorer choose integer 1 to 6 to represent 6 different levels of essays, but for the computers, after so many calculations, it is quite reasonable that it can not give score in the form of integer. However, each essay is given a different score, and therefore classified. Score between 0.5 to1.5 is classified as level 1, 1.5 to 2.5 is level 2; 2.5 to 3.5 is level 3; 3.5 to 4.5is level 4; 4.5 to 5.5; 5.5 to6.5 is level 6.

In Table-2, we can see that 27 essays are correctly scored, so the correction rate is 67.5%. Considering the number of essays used in training is limited, the result is quite acceptable.

5. FUTURE WORK

The method stated above does not involve any detection of mistakes in spelling English words and grammar usage. By connecting a database, we can make this possible and we can score the vocabulary usage more precisely. Although giving a word score according to its number of syllables is a general rule, some short words are also quite advance and should be given a higher score.

The method also lacks the analysis of semantic content of the essay. In this method, for instance, an example will add score to the essay's content, no matter how well it can support the author's opinions. Future work involving the semantic analysis of the essay can improve the precision of the essay's score; at least nonsense should be detected.

Lastly, enlarging the number of essays used as samples for training and testing will also improve the performance of this method.

ACKNOWLEDGEMENTS

The research is supported by Undergraduate Innovative Research Training program and Undergraduate Open Lab Project of Wuhan University of Technology. No: KF023, A107.

REFERENCES

[1] Sugiyama M, Ogawa,H, "Incremental projection learning for optimal generalization," NeuralNetworks, 2001, 14(1);3-56

[2] John Langan, College Writings Skills With Readings, 2002

[3] Burstein, Jill, Marcu, Daniel, and Knight, 'Kevin Finding the WRITE Stuff:Automatic Identification of Discourse Structure in Student Essays," *Special Issue on Natural Language Processing of IEEE Intelligent Systems*, January/February, 2003.

[4] Derrick Higgins Jill Burstein Daniel Marcu Claudia Gentile Evaluating Multiple Aspects of Coherence in Student Essays 2003.

[5] Derrick Higgins Jill Burstein Sentence similarity measures for essay coherence 2003.

[6] SJ Russell, P Norving, Artificial Intelligence: A modern approach, 2003.

[7] Jill Burstein Magdalena Wolska Toward Evaluation of Writing Style: Finding Overly Repetitive Word Use in Student Essays.2004.

[8] MR Genesereth, NJ Nilsson, Logical Foundations of artificial intelligence 2000.

[9] Jill BURSTEIN Daniel MARCU Benefits of Modularity in an Automated Essay Scoring System 2005.

[10] F. L. LU O and R. U NBEHAU EN Applied Neural Networks for Signal Processing 2002.

Wei Weng was born in1986. He is currently an undergraduate in the school of computer science and technology, Wuhan University of Technology. His research interests include artificial intelligence and distributed computing.

Dewei Peng was born in 1976. He received the BE and ME degree in Wuhan University, China, in 1998 and 2001, respectively. He is currently a associate professor in the Department of Computer Science and Technology, wuhan university of technology, China. His research includes mobile agent, distributed computing and artificial intelligence.

Chaotic Time Series Forecasting with QPSO-Trained RBF Neural Network

Wenbo Xu, Jun Sun
Center of Intelligent and High Performance Computing,
School of Information Technology, Southern Yangtze University
Wuxi, Jiangsu 214122, China
Email: xwb_sytu@hotmail.com

ABSTRACT

Radial Basis Function (RBF) networks are widely applied in function approximation, system identification, chaotic time series forecasting, etc. To use a RBF network, a training algorithm is absolutely necessary for determining the network parameters. In this paper, we use Quantum-behaved Particle Swarm Optimization (QPSO), a newly proposed evolutionary search technique, to train RBF neural network and therefore apply QPSO-trained RBF network in chaotic time series forecasting. The proposed method was test on Mackey-Glass model, and the results show that it can predict the time series more quickly and precisely than the RBF network trained by Particle Swarm Optimization (PSO) algorithm.

Keywords: Quantum-behaved PSO, RBF

1. INTRODUCTION

Radial Basis Functions emerges as a variant of feed-forward artificial neural network in late 80's. They are function approximation models that can be trained by examples to implement a desired input-output mapping. Due to their excellent nonlinear approximation properties, RBF neural networks are able to model complex mappings, which perceptron neural networks can only model by means of multiple intermediary layers [11]. RBF networks have been successfully applied to a large diversity of applications including interpolation [4], chaotic time-series modeling [5], system identification [15], etc.

In order to use a Radial Basis Function network we need to specify the hidden unit activation function, the number of processing units, a criterion for modeling a given task and in turn, a training algorithm for finding the parameters of network. Finding the RBF weight is called network training. If we have at hand a set of input-output pairs, called training set, we optimize the network parameters in order to fit the network outputs to the given inputs. The fit is evaluated by means of a cost function, usually assumed to be the mean square error. After training, the RBF can be used with data whose underlying statistics is similar to that of the training set.

The most widely used training algorithms for RBF network include Orthogonal Least Squares (OLS) algorithm, clustering and gradient-based algorithm, etc. These algorithms, however, possess their shortcomings, which will be mentioned in Section 2. Evolutionary algorithms are a class of population-based search techniques, which have strong global search ability and robustness and could be used to training RBF and other neural networks. They can solve difficult problems with objective functions that do not possess "nice properties" such as continuity, differentiability, satisfaction of the Lipshcitze Condition, etc. Due to these excellences, evolutionary algorithm becomes promising training algorithm for neural networks.

Particle Swarm Optimization is a newly proposed evolutionary approach, which differs from other evolution-motivated evolutionary computation in that it is motivated from the simulation of social behavior. PSO can be easily implemented but is computationally inexpensive. The method requires only the function value, and does not require gradient information of the objective function of the global optimization problem under consideration. On the other hand only primitive mathematical operators are used. Hence the method requires low memory and small computational requirement.

Recently, a novel and global convergent variant of PSO, Quantum-behaved Particle Swarm Optimization (QPSO), has been proposed [17-19]. It has been shown that QPSO outperforms PSO considerably in several benchmark function optimization. In this paper, we will apply QPSO in training RBF neural network and thus use QPSO-trained RBF network to predict chaotic time series. The paper is structured as follows. In Section 2 and 3, RBF network model and parameter selection problem are introduced. Section 4 describes QPSO algorithm. In Section 5, we propose our QPSO-Trained RBF network model. The problem of chaotic time series forecasting is described in Section 6. Section 7 gives the experiments results of the proposed model on a well-known testing problem. Finally, the paper is concluded in Section 8.

2. STRUCTURE OF RBF NEURAL NETWORK

RBF Neural Network is structured by embedding radial basis function a two-layer feed-forward neural network. Such a network is characterized by a set of inputs and a set of outputs. In between the inputs and outputs there is a layer of processing units called hidden units. Each of them implements a radial basis function. The architecture of RBF network is shown in Fig.1.

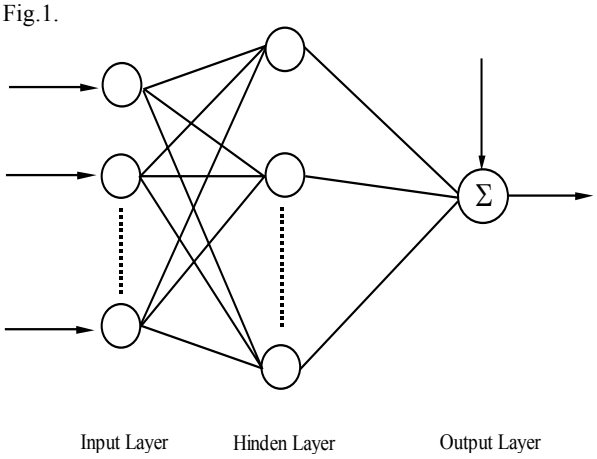


Fig.1. RBF network in time series modeling

Mathematically the RBF network can be formulated as:

$$g(x)=\sum_{k=1}^{m}\lambda_k\varphi_k\left(\|x-c_k\|\right) \tag{1}$$

where m is the neuron number of hidden layer, which is equal

to cluster number of training set. $\|x-c_k\|$ stands for the distance between the data point x and the RBF center c_k. λ_k is the weight related with RBF center c_k. Therefore, the RBF neural networks output is a weighted sum of the hidden layer's activation functions. Various functions have been tested as activation functions for RBF networks. In this paper, we adopt the most commonly used Gaussian RB functions as basis functions, then in the formula (1),

$$\varphi_k(x) = \frac{R_k(x)}{\sum_{i=1}^{m} R_i(x)} \quad (2)$$

$$R_k(x) = \exp\left(-\frac{\|x-c_k\|^2}{2\sigma_k^2}\right) \quad (3)$$

In formula (3), σ_k indicates the width of the kth Guassian RB functions. One of the σ_k selection methods is shown as follows.

$$\sigma_k^2 = \frac{1}{M_k} \sum_{x\in\theta_k} \|x-c_k\|^2 \quad (4)$$

where θ_k is the kth cluster of training set and M_k is the number of sample data in the kth cluster.

3. PARAMETER SELECTION OF RBF NEURAL NETWORK

The neuron number of the hidden layer, i.e., the cluster number of training set, must be determined before the parameter selection of RBF neural network. In this paper, we adopt an efficient method, Rival Penalized Competitive Learning (RPCL) [24], to decide the cluster number.

If the neuron numbers of hidden layer has been decided, the performance of RBF depends on the selection of the network parameters. There are three types of parameters in a RBF neural network model with Gaussian basis functions:

(1) RBF centers (hidden layer neurons),
(2) Widths of RBFs (standard deviations in the case of a Gaussian RBF)
(3) Output layer weights

Different strategies exist for training of RBF neural network models. By means of training, the neural network models the underlying function of a certain mapping. In order to model such a mapping we have to find the network weights and topology. There are two categories of training algorithms: supervised and unsupervised. RBF networks are used mainly in supervised applications. In a supervised application, we are provided with a set of data samples called training set for which the corresponding network outputs are known. In this case the network parameters are found such that they minimize a cost function. In unsupervised training the output assignment is not available for the given set.

A large variety of training algorithms has been tested for training RBF networks. In the initial approaches, to each data sample was assigned a basis function. This solution proved to be expensive in terms of memory requirement and in the number of parameters. On the other hand, exact fit to the training data may cause bad generalization. Other approaches choose randomly or assumed known the hidden unit weights and calculate the output weights λ_{jk} by solving a system of equations whose solution is given in the training set [4]. The matrix inversion required in this approach is computationally expensive and could cause numerical problems in certain situation (when the matrix is singular). In [15], the radial basis function centers are uniformly distributed in the data space. The function to be modeled is obtained by interpolation.

Orthogonal least squares using Gram-Schmidt algorithm is proposed in [6]. An adaptive training algorithm for minimizing a given cost function is gradient descend algorithm. Backpropagation adapts iteratively the network weights considering the derivatives of the cost function with respect to those weights [10]. Backpropagation algorithm may require several iterations and can get stuck into a local minimum of the cost function (4). Clustering algorithms such as k-means [22], or learning vector quantization [9] have been employed for finding the hidden unit parameters in [26]. The centers of the radial basis functions are initialized randomly. This algorithm is online and its first stage is unsupervised. For a given data sample X_i, the algorithm adapts its closest center.

The training algorithms mentioned have their own shortcomings respectively. In the existing literature, many attempts have been made to employ evolutionary computing approaches, such as Genetic Algorithm (GA) and PSO, to train RBF as well as other neural networks. For instance, in [11], Juang propose a hybrid of GA and PSO for the design of recurrent neural network. In the rest part of the paper, we will present how to train RBF neural network by the newly proposed QPSO.

4. QUANTUM-BEHAVED PARTICLE SWARM

Particle Swarm Optimization (PSO) algorithm is a population-based optimization technique originally introduced by Kennedy and Eberhart in 1995 [12]. A PSO system simulates the knowledge evolvement of a social organism, in which each individual is treated as an infinitesimal particle in the n-dimensional space, with the position vector and velocity vector of particle i being represented as $X_i(t)=(X_{i1}(t),X_{i2}(t),\cdots,X_{in}(t))$ and $V_i(t)=(V_{i1}(t),V_{i2}(t),\cdots,V_{in}(t))$. The particles move according to the following equations:

$$V_{ij}(t+1)=V_{ij}(t)+c_1\cdot\eta\cdot(P_{ij}(t)-X_{ij}(t))+c_2\cdot r_2\cdot(P_{gj}(t)X_{ij}(t)) \quad (5)$$

$$X_{ij}(t+1)=X_{ij}(t)+V_{ij}(t+1) \quad i=1,2,\cdots M;\ j=1,2\cdots,n$$

where c_1 and c_2 are called the acceleration coefficients. Vector $P_i=(P_{i1},P_{i2},\cdots,P_{in})$ is the best previous position (the position giving the best fitness value) of particle i known as the personal best position (pbest); vector $P_g=(P_{g1},P_{g2},\cdots,P_{gn})$ is the position of the best particle among all the particles in the population and is known as the global best position (gbest). The parameters η and r_2 are two random numbers distributed uniformly in (0,1), that is $\eta, r_2 \sim U(0,1)$. Generally, the value of V_{ij} is restricted in the interval $[-V_{max}, V_{max}]$.

Many revised versions of PSO algorithm are proposed to improve the performance since its first introduction in 1995. Two most important improvements are the version with an Inertia Weight [23], w, and a Constriction Factor [7], K. In the inertia-weighted PSO the velocity is updated by using

$$V_{ij}(t+1)=w\cdot V_{ij}(t)+c_1\cdot\eta(P_{ij}(t)-X_{ij}(t))+c_2\cdot r_2\cdot(P_{gj}-X_{ij}(t)) \quad (6)$$

While in the Constriction Factor model the velocity is obtained by using

$$V_{ij}(t+1)=K\cdot(V_{ij}(t)+c_1\cdot r_2\cdot(P_{ij}(t)-X_{ij}(t))+c_2\cdot r_2\cdot(P_{gj}-X_{ij}(t))) \quad (7)$$

While in the Constriction Factor model the velocity is obtained by using

$$V_{ij}(t+1)=K\cdot(V_{ij}(t)+c_1\cdot r_2\cdot(P_{ij}(t)-X_{ij}(t))+c_2\cdot r_2\cdot(P_{gj}-X_{ij}(t))) \quad (8)$$

Where

$$K=\frac{2}{\left|2-\varphi-\sqrt{\varphi^2-4\varphi}\right|},\quad \varphi=c_1+c_2,\quad \varphi>4 \tag{9}$$

There exists another general form of particle swarm, referred to as the LBEST method in [16]. This approach divides the swarm into multiple "neighborhoods", where each neighborhood maintains its own local best solution. This approach is less prone to becoming trapped in local minima, but typically has slower convergence. Kennedy has taken this LBEST version of the particle swarm and applied to it a technique referred to as "social stereotyping" [13].

Trajectory analyses in [8] demonstrated the fact that convergence of the PSO algorithm may be achieved if each particle converges to its local attractor. Let the local attractor $p_i=(p_{i1},p_{i2},\cdots p_{iD})$ be defined at the coordinates

$$p_{ij}(t)=(c_1\eta P_{ij}(t)+c_2r_2P_{gj}(t))/(c_1\eta+c_2r_2),\quad 1\le j\le n \tag{10}$$

which is re-written as

$$p_{ij}(t)=\varphi\cdot P_{ij}(t)+(1-\varphi)\cdot P_{gj}(t),where\quad \varphi=c_1\eta/(c_1\eta+c_2r_2) \tag{11}$$

Eqn (11) consists of only one random number. It can be seen that the local attractor is a stochastic attractor of particle i that lies in a hyper-rectangle with P_i and P_g being two ends of its diagonal, and moves according to P_i and P_g

In QPSO, each individual particle moves in a search space with a Delta Potential Well in each dimension, whose center is p_{ij}. Solving Schrödinger equation for each dimension, we can get the probability distribution function D is

$$D(|p_{ij}-X_{ij}|)=e^{-2|p_{ij}-X_{ij}|/L} \tag{12}$$

Using Monte Carlo method, we can get

$$X_{ij}=p_{ij}\pm\frac{L}{2}\ln(1/u) \tag{13}$$

The value of L and the position are evaluated by

$$L=2\alpha\cdot|C_j(t)-X_{ij}(t)| \tag{14}$$

where C_j is the jth component of a global point called Mainstream Thought or Mean Best Position (mbest) of the swarm population, which is defined as the mean of the personal best positions among all particles.

$$C(t)=(C_1(t),C_2(t),\cdots,C_D(t))=\left(\frac{1}{M}\sum_{i=1}^{M}P_{i1}(t),\ \frac{1}{M}\sum_{i=1}^{M}P_{i2}(t),\ \cdots,\ \frac{1}{M}\sum_{i=1}^{M}P_{iD}(t)\right), \tag{15}$$

$$X_{ij}(t+1)=p_{ij}(t)\pm\alpha\cdot|C_j(t)-X_{ij}(t)|\cdot\ln(1/u) \tag{16}$$

QPSO Algorithm

```
Initialize particles with random position Xi=X[i][:];
Initial approximation of personal best position Pi=Xi;
while stop criterion is not met do
    Compute the mean best position C[:] by equation (15);
    for i = 1 to swarm size M
        If f(Xi)<f(Pi) then Pi=Xi; endif
        Find the Pg=P[g][:]by equation;
        for j=1 to D
              =rand(0,1); u=rand(0,1);
          p=φ*P[i][j]+(1-φ)*P[g][j];
           if(rand(0,1)>0.5
            X[i][j]=
              p+α*abs(C[j]-X[i][j])*ln(1/u);
           Else
            X[i][j]=
              p-α*abs(C[j]-X[i][j])*ln(1/u);
           Endif
        Endfor
    Endfor
Endwhile
```

In the QPSO, the parameter must be set as $\alpha<1.782$ to guarantee convergence of the particle [19]. Generally, the value of . no more than 1.0 can lead to a good performance if it is fixed over the running of QPSO. But in most cases, decrease linearly from α_0 to α_1 ($\alpha_0<\alpha_1$).

5. QPSO-TRAINED RBF NEURAL NETWORK

When training RBF neural network by QPSO, a decision vector represents a particular group of network parameters including c_k, λ_k and c_k $(k=1,2,\cdots,m)$. Thus each particle flies in a 3m-dimensional search space with $X_i=(c_1,c_2,\cdots,c_m,\sigma_1,\sigma_2,\cdots,\sigma_m,\lambda_1,\lambda_2,\cdots,\lambda_m)$ denoting its position. Initialization of the population involves generating randomly the position vector X_i $(i=1,2,\cdots,M)$ and setting the personal best position $P_i=X_i$ $(i=1,2,\cdots,M)$.

Since a component of the position corresponds to a network parameter, a RBF network is structured according the particle's position vector. Training the corresponding network by inputting the training samples, we can obtain an error value computed by the following formula.

$$E=\frac{1}{2Q}\sum_{j=1}^{Q}\sum_{s=0}^{c}[y_{s,j}(x_j)-g_{s,j}(x_j)]^2 \tag{17}$$

where $y_{s,j}(x_j)$ and $g_{s,j}(x_j)$ are the actual response (output) and network's predicted response (output) at output unit s on x_j, respectively. Q is the number of the training sample and c is the number of output units. The particle is evaluated by the obtained error value (fitness value), by which it can be determined whether P_i and P_g need to be updated. In a word, the error function (17) is adopted as the objective function to be minimized in QPSO-based RBF neural network.

There are two alternatives for stop criterion of the algorithm. One method is that the algorithm stops when the increment of objective function value is less than a given threshold ε; the other is that it terminates after executing a pre-specified number of iterations. The following is the description of QPSO-Trained RBF neural network algorithm:

(1) Initialize the population by randomly generate the position vector X_i of each particle and set $P_i=X_i$;
(2) Structure a RBF neural network by treating the position vector of each particle as a group of network parameter;
(3) Training each RBF network on the training set;
(4) Evaluate the fitness value of each particle by formula (19), update the personal best position P_i and obtain the global best position P_g across the population;
(5) If the stop criterion is met, go to step (7); or else go to step (6);
(6) update the position vector of each particle according to (18);
(7) Output the P_g as a group of optimized parameters.

6. CHAOTIC TIME SERIES FORECASTING BY QPSO –TRAINED RBF

Assume that $x(k),k=1,2,3,\cdots$ is a chaotic time series, the purpose of chaotic time series forecasting is to determine $x(k+p)$ when $x(k-m+1)$, $x(k-m+2),\cdots,x(k)$ are given. In this paper, the problem is reduced to, based on the given sample data $x(1),x(2),...,x(M)$, constructing $M-m-p+1$ pairs of input-output data: $[x(M-m-p+1),...,x(M-p);x(M)]$, $[x(M-m-p),...,x(M-p-1);x(M-1)]$, $[x(1),...,x(m);x(m+p)]$, that is, constructing input-output pairs $[x(n);d(n)],n=1,2,...,N$, where $x(n)=(x_1(n),...,x_m(n))\in R^m$ represent m inputs of the system under consideration, $d(n)\in R$ is the expectant response of the system and N is the number of sample data (sample size).

In the process of forecasting chaotic time series by RBF network, the first l input-output pairs in the sample data are employed as training set to establish the chaotic time series forecasting model based on RBF network and the last N-l pairs are used as testing data to test the times series.

7. EXPERIMENTS

In this paper, we used Mackey-Glass Model described following as the testing system.

$$\frac{dx(n)}{dn}=\frac{0.2*x(n-\tau)}{1+x^{10}(n-\tau)}-0.1*x(n) \qquad (18)$$

The system comes into chaotic state when $\tau>17$. In our experiment, we set $\tau=30$ and $x(0)=0.6$. Therefore we may work out chaotic time series numerically. In the process of forecasting as described in the above section, we set $m=4$ and $p=1$. When testing Mackey-Glass Model, we set $M=1004$ and thus construct N=1000 sample data pairs, of which the first 800 pairs are used as training set and the last 200 as testing data.

We use PSO and QPSO as training algorithm for RBF network respectively for performance comparison. The experiment configuration is as follows. For PSO, the inertial weight ω varies linearly from 0.9 to 0.4 over the running of the algorithm, the acceleration coefficients c_1 and c_2 are both set to 2 and Vmax is 15; For QPSO, the CE coefficient varies linearly from 1.0 to 0.5 over the running. Both the training algorithms use 20 particles and execute for 200 iterations. The RBF network used in our experiment has 4 input neurons, 8 neurons in hidden layer and one output neuron.

The experiment results are shown in Fig 2 and Fig 3, where Fig 2 is the visualization of the results on training set and Fig 3 is that of the results on testing data. It can be seen that RBF network trained by either QPSO or PSO can predict the chaotic time series with high precision. More concretely, when tested on testing data, QPSO-trained RBF network yields mean error 0.001877 averaged over 50 runs, while PSO-trained RBF generates mean error 0.002116. It means that the chaotic times series could be forecasted more precisely by the RBF network trained by QPSO, due to the stronger search ability of the algorithm.

We also visualized in Fig 4 the convergence processes of QPSO and PSO when they are training RBF networks. The results recorded are averaged over 50 runs. It can be seen from Fig 4 that QPSO converges to the global optima more quickly than PSO in the whole stage of the search.

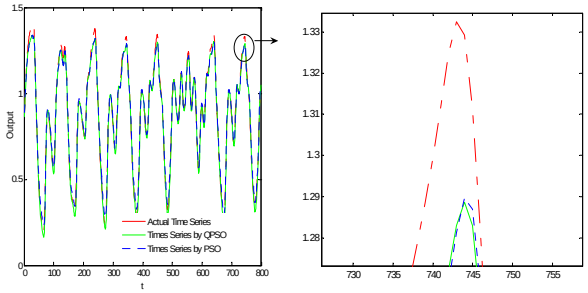


Fig. 2. Experiment results on training set.

8. CONCLUSIONS

In this paper, we employ the newly proposed QPSO to train RBF network and use QPSO-trained RBF neural network to forecast chaotic time series. The experiment results of QPSO-Trained RBF network on the testing problem show that it can predict the chaotic time series more quickly and precisely than the RBF network trained by PSO thanks to the stronger search ability of QPSO.

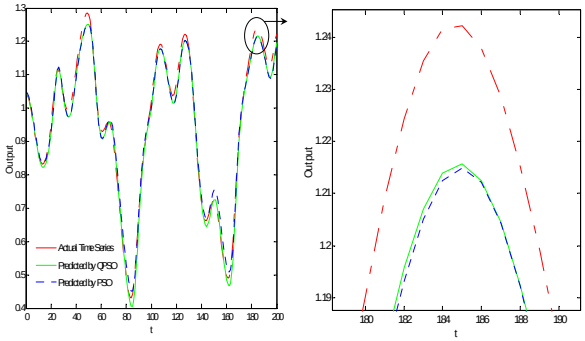


Fig. 3. Experiment results on testing data

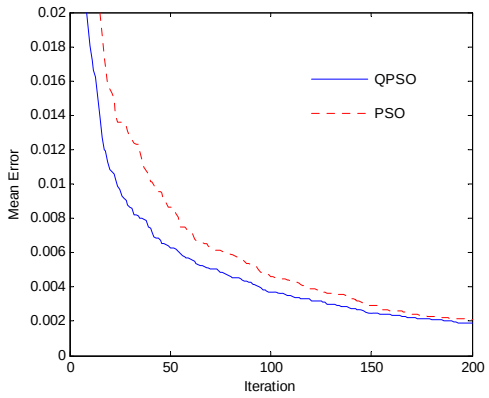


Fig. 4. Convergence processes of QPSO and PSO both averaged over 50 runs.

Although QPSO is also an evolutionary population-based search technique like PSO, it is a global convergent algorithm while PSO is not. Therefore, QPSO can find out the global optima of the optimization problem at more easily and more quickly. Our future work will focus on applying QPSO to training other neural network and use QPSO-Trained RBF in real world applications.

REFERENCES

[1] P. J. Angeline, "Evolutionary Optimization Versus Particle Swarm Optimization: Philosophy and performance Differences," Evolutionary Programming VII (1998), *Lecture Notes in Computer Science* 1447, pp. 601-610, Springer.

[2] F. Van den Bergh, A. P. Engelbrecht, "A New Locally Convergent Particle Swarm Optimizer," 2002 IEEE International Conference on systems, Man and Cybernetics, 2002.

[3] F. Van den Bergh, "An Analysis of Particle Swarm Optimizers," PhD Thesis. University of Pretoria, Nov 2001.

[4] D.S. Broomhead, D. Lowe, "Multivariable Functional Interpolation and Adaptive Networks", Complex Systems, vol. 2, pp. 321-355.

[5] M. Casdagli, "Nonlinear Prediction of Chaotic Time Series", *Physica D*, vol. 35, pp. 335-356.

[6] S. Chen, C.F.N. Cowan and P.M. Grant "Orthogonal Least Squares Learning Algorithm for Radial Basis Function Networks", *IEEE Trans. On Neural Networks*, 1991, vol.2, no.2, pp.302-309.

[7] M. Clerc, "The Swarm and Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," *Proc. Congress on Evolutionary Computation 1999*, pp. 1951-1957.

[8] M. Clerc and J. Kennedy, "The Particle Swarm: Explosion, Stability, and Convergence in a Multi-dimensional Complex Space", *IEEE Transaction on Evolutionary Computation*, no. 6, pp. 58-73, 2002.

[9] T.K. Kohonen, *Self-Organization and Associative Memory*. 1989, Berlin: Springer-Verlag.

[10] S. Haykin, "Neural Networks: A Comprehensive Foundation", *Upper Saddle River*, NJ: Prentice Hall

[11] C.F. Juang, "A Hybrid of Genetic Algorithm and Particle Swarm Optimization for Recurrent Network Design", *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS*, VOL. 34, NO. 2, APRIL 2004, pp. 997-1006.

[12] J. Kennedy, R. C. Eberhart, "Particle Swarm Optimization," *Proc. IEEE Int'l Conference on Neural Networks*, IV. Piscataway, NJ: IEEE Service Center, 1995, pp. 1942-1948.

[13] J. Kennedy, "Sereotyping: Improving Particle Swarm Performance with cluster analysis," in *Proc. 2000 Congress on Evolutionary Computation*, pp. 1507-1512.

[14] J. Kennedy, "Small worlds and Mega-minds: Effects of Neighborhood Topology on Particle Swarm Performance," *Proc. Congress on Evolutionary Computation 1999*, pp. 1931-1938.

[15] R. M. Sanner, J.-J. E. Slotine, "Gaussian Networks for Direct Adaptive Control", *IEEE Trans. On Neural Networks*, vol.3, no.6, pp.837-863.

[16] P. N. Suganthan, "Particle Swarm Optimizer with Neighborhood Operator," *Proc. 1999 Congress on Evolutionary Computation*, pp. 1958-1962.

[17] J. Sun et al, "Particle Swarm Optimization with Particles Having Quantum Behavior," *Proc. 2004 Congress on* Evolutionary *Computation*, pp. 325-331.

[18] J. Sun et al, "A Global Search Strategy of Quantum-behaved Particle Swarm Optimization," *Proc. 2004 IEEE Conference on Cybernetics and Intelligent Systems*.

[19] J. Sun et al, "Adaptive Parameter Control for Quantum-behaved Particle Swarm Optimization on Individual Level", *Proceedings of 2005 IEEE International Conference on Systems, Man and Cybernetics*, pp. 3049-3054.

[20] J. Vesterstrom, J. Riget and T. Krink: "Division of Labor in Particle Swarm Optimization". *IEEE 2002 Proceedings of the Congress on Evolutionary Computation*.

[21] Y. Shi and R. Eberhart, "Empirical Study of Particle Swarm optimization," *Proc. of Congress on Evolutionary Computation*, 1999, 1945-1950.

[22] J.T. Tou and R.C. Gonzalez, *Pattern Recognition. Reading*, MA: Addison-Wesley.

[23] Y. Shi, R. C. Eberhart, "A Modified Particle Swarm," *Proc. 1998 IEEE International Conference on Evolutionary Computation*, pp. 1945-1950.

[24] L. Xu et al,"Rival Penalized Competitive Learning for Clustering Analysis,RBF Net,and Curve Detection", *IEEE Trans on Neural Networks*, 1993, 4(4), pp. 636-649

[25] X.B.Yang etal, "Time Series Forecasting with RBF Neural Network", *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics,* pp. 4680-4683, Guangzhou, 18-21 August 2005.

Wenbo Xu, male, Full Professor, his research interests are in the artificial intelligence, the computer control, inserts the type operating system, the parallel computation, the pattern recognition;

Jun Sun, male, doctor graduate student, his research interests are in financial computation, evolution computation.

Combinations of Neural Networks and Other Intelligent Methods*

Luo Zhong, Cuicui Guo
School of Computer Science and Technology, WuHan University of Technology
Wuhan, 430070, China
Email: guocc@whut.edu.cn

ABSTRACT

As an important part in AI, technique of neural networks has been applied in many fields successfully. But in corporate symbol computation system, each one of intelligent technique could just reinforce each other. It is becoming a focus of attention that how to effectively combine these intelligent methods with neural networks to attain the aim of learning from others' strong points to offset one's weakness. This article will discuss some methods in combinations of intelligent methods with neural networks technology and its execution possibility on theory.

Keywords: Combination, Intelligent Methods, Neural Networks, Expert Systems, Fuzzy Logic, CMGA, Wavelet Analysis, Chaos, Rough Sets, Fractal Theory

1. INTRODUCTION

In corporate symbol computation system, each one of intelligent technique could just reinforce each other. So how to effectively combine these intelligent methods with NN is becoming a hot topic. It is practically meaningful to combine these techniques forming an intelligent application system, which either contain both advantages, synergetic or integrated. In recent years, considering the protruding characters of NN, such as distributed storing, parallel processing, self-learning and organizing, and non-linear mapping, more and more are discussing and doing research on combinations with expert systems, fuzzy logic, genetic algorithms, wavelet analysis, chaos, rough sets, and fractal theory.

2. COMBINATIONS OF NEURAL NETWORKS AND EXPERT SYSTEMS

Most expert systems are good at logic inferring and symbol information processing. But its own deficiency limited its development. If realizing details of expert systems and NN are not taken into account, both of the two techniques have common beginnings and goals. Therefore, certain advantages of neural networks can compensate the deficiency of expert systems and enhance the capability of the systems at the same time[2]. Three ways of combining neural networks and expert systems are as following:

2.1 Neural Networks based Expert Systems

In this kind of systems architecture, its part or all functions were realized by neural networks, the advantage lies in the capability of learning and adapting. It also avoids most difficulties in knowledge acquisition procedure, but its disadvantage lies in unable to explain inference procedure and basis. Inputs are usually examples of engineering project, and knowledge acquisition procedure will be done by NN, there is no use summarizing and inducing by project engineer.

* Project (No.2004XD-03) supported by ministry of education's action planning project.

2.2 Knowledge based Neural Networks Systems

It is also called expert networks, for taking expert system as its event driven. Neural units represent the premise and conclusion of expert system, connection weights represent certain elements of expert system, and its own network architecture keeps the same as rule sets of expert system above [8]. In this mode, there are AND, OR and NOT operators in systems, then rule sets of expert systems can be reflected as expert networks. As Fig.1 show, the weight 1 can not be modified, so it is also called hard-weight, oppositely, other weights which can be modified are called soft-weight.

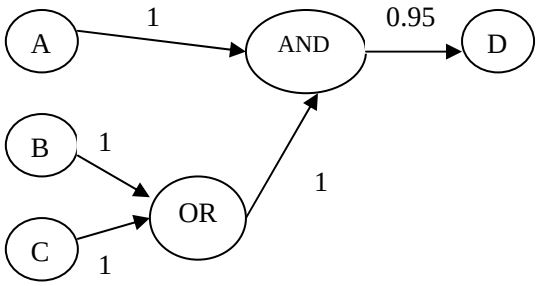


Fig.1. RULE: IF A AND (B OR C) THEN D

2.3 Mixed System of Neural Networks and Expert Systems based

Classifying the whole complex system into each functionally part module is the foundation purpose, and each one will be realized by either neural networks or expert systems. The problems ranked the top are frame designing and rules selecting of realizing functional subsystem [4]. In fact, these two problems consist of a whole one and can not be separated.

One point of view comes from the application consideration, for subsystem which we can easily understand its rules equation will be realized by expert technique, and other part will be done by neural networks, in this way, the architecture will change along with the real problem.

The other point of view lies in the function needs, for instance, using neural networks to realize the rules inducing procedure and knowledge acquisition procedure in an expert system, meanwhile, expert system will responsible for the representation of knowledge and evaluation and explanation of results.

3. COMBINATIONS OF NEURAL NETWORKS AND FUZZY LOGIC

Nowadays, in our country, fuzzy logic controlling technique used in fields like industry controlling and family electronics develops very quickly, and scientists are focusing almost all of their efforts on creating appropriative fuzzy controlling circuitries and fuzzy inference chips. While readability is

remain the chief character of a fuzzy logic system, at the same time neural networks has strong self-learning capability. There are three ways of combining fuzzy logic with neural networks technology.

3.1 Applying Fuzzy Logic to Neural Networks

Applying fuzzy logic to neural networks is mainly using the concept of fuzzy sets in neural networks' computing and learning procedures, as a result, to enhance the learning performance of the neural networks obviously.

3.2 Applying Neural Networks to Fuzzy Systems

In applying neural networks to fuzzy system, one choice is using the learning capability of neural networks to extend real knowledge warehouse, along with the enhancement of maintainability [5]. The other one is realizing a given fuzzy system by neural networks technology, to complete the meantime fuzzy inference of this system.

3.3 Mixed System of Neural Networks and Fuzzy Logic based

Fusion ways refers to using the architecture of neural networks to finish fuzzy inference procedure, meanwhile, improve the acquisition and modification capability of knowledge. In this way, both advantages of neural networks and fuzzy system can be attained.

4. COMBINATIONS OF NN AND CMGA (CONTRACTIVE MAPPING GENETIC ALGORITHMS)

Genetic algorithm was first introduced by Holland [1] in year 1962. It was a wholly optimization searching algorithm based on natural selection theory and genetic inheritance theory. For it is simple, robust and easy parallel processing, more and more complex problems are taking this idea to solve real world questions [7]. For classic genetic algorithm can not guarantee general optimization convergence, based on professor Bnanach's theory (1927), construct appropriate measurement space S, make sure that GA in this scale is convergent, then any contractive mapping f has the only stable point. Meanwhile, we can get the possibility of convergence on this point, not to associate with the selection of original swarm [3].

The combining of the two techniques lies in using contractive mapping genetic algorithms to train BP neural network. Under consideration of the theory described above, based on CMGA, BP neural networks can get an optimization convergence and weights training won't lie in original weights selection. Therefore, the veracity of representing relations among variables will get prompted, and time consuming of training will be also less.

Designing and practicing of neural networks based on evolutionary computing are playing an important role in most fields, such as pattern identifying, robot controlling, and financial predicting and so on. The implementation results say that it is a better way solving problems than traditional neural networks technology.

5. COMBINATIONS OF NEURAL NETWORKS WITH WAVELET ANALYSIS, CHAOS, ROUGH SETS, AND FRACTAL THEORY

5.1 Combinations with Wavelet Analysis

From year 1986, based on foundation work of Y.Meyer, S.Mallat and I.Daubechies, wavelet analysis develops very quickly and become a booming subject. Meyer's work "wavelet and operator" and Daubechies's "ten lessons about wavelet" are the most powerful works in wavelet fields.

Wavelet transformation has a better local timing-frequency, combing with self-learning capability of neural networks, formed a more powerful approaching and error containing capability wavelet neural network. In combing ways, wavelet functions can be used as base-function constructing wavelet neural networks, or as a pre-input processing tool imposed on state signal. At the same time, it can pick up the prior characters as inputs for wavelet neural networks.

5.2 Combinations with Chaos Theory

In year 1990, K.Aihara, T.Takabe and M.Toyada etc. first introduced chaos neural networks model, making that artificial neural network has chaos behavior, approaching to real brain's neural networks. Therefore, chaos neural networks are regarded as one of the intelligent information processing systems which can reflect the real world. After that, it becomes a main braches for more and more researchers.

Comparing with standard discrete Hopfield neural networks, chaos neural network has a prominent non-linear kinetic character, for instance, the synchronous character for chaos neural networks, magnetizing operators. To make sure that chaos phenomena are operating under control, more work are to do with revising and adjusting architectures of chaos neural networks, and more researches on neural networks algorithms.

5.3 Combinations with Rough Sets

Rough sets theory was first introduced by professor Z.Pawlak in year 1982. It is a kind of mathematical theory used for analyzing datum, representing, learning and inducing incomplete datum and incomplete knowledge. Rough sets theory was a newly tools aimed for processing fuzzy and uncertain knowledge. Its core idea lies in premising that holding classification ability, through knowledge reduction, concluding strategy for problems and rules for classifying.

Therefore, combining rough sets with neural networks is a feasible way of prompting the whole systems efficiency. Using rough sets method to processing information beforehand, namely taking rough sets network as pre-system, then based on information structure after above step, a neural network information processing system will be constructed. From this way, the number of attributes will be less, the complexity of the whole system will be reduced and the whole new system will has a strong anti-jamming ability. It is a powerful way for processing uncertain and incomplete information.

5.4 Combinations with Fractal Theory

After introducing the concept fractal by Harvard professor B.B.Mandelbrot in 1970s, fractal geometry developed as one of the scientific methodologies-fractal theory, and also regarded as opening up an important phase for mathematic development. It is widely used in scientific and social fields, becoming a foreland topic nowadays.

It is prominent that Using fractal theory to explain the abnormal, unstable and highly complex phenomena. Meanwhile, combing neural networks with fractal theory can take fully use of neural networks' non-linear mapping function, calculation ability, self-adjusting ability, a better result will be attained.

6. CONCLUSIONS

Although neural networks technology has been applied in many fields successfully, but there is still a big space to develop it and perfect it. For example, deeper research on fundamental theory of neural computation frame, biological activities of people, also on new model and architecture, readability of neural networks, and better combination applications of neural networks with other techniques. Future research activities should put hands on new method and new technology of each aspect of people's daily life. Shrilling out advantages of each technique and combining them effectively to form a better method than single one technique. Making it used more widely and more effectively in more scientific fields [6].

REFERENCES

[1] Holland J. H., *Adaptation in Nature and Artificial System*. Ann Arbor: Univ. of Michigan Press,1975.

[2] L. Zhong, C. M. Zou, "The Research of System Architecture in Expert System," *Wuhan University Journal of Natural Science*, 2001,16(1-2).

[3] Kenneth O. S. and Risto, M. , "Efficient Reinforcement Learning through Evolving Neural Network Topologies," in *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO-2002)*, Morgan Kaufmann, USA, 2002.

[4] Medsker L R .,*Hybrid Neural Networks and Expert Systems*. Boston Kluwer Academic Publisher, 1994.

[5] L. Zhong, "Researching of Forward Generating Neural Network," *Proc. of Inter. Conf. on Sensors and control Techniques*, SPIE, Vol.4077,USA, 2000.

[6] L. Zhong, L. S. Liu, etc, "The Application of Neural Network in Lifetime Prediction of Concrete," *J. of Wuhan University of Technology*, 2002,17(1).

[7] Dimopoulos, C. and Zalzala, A. M. S., "Recent Development in Evolutionary Computation for Manufacturing Optimization: Problems, Solutions, and Comparisons," *IEEE Transactions on Evolutionary Computation*, vol.4 (2), pp.93-113, 2000.

[8] L. Zhong, etc., "A Study of Dynamic Knowledge Representation Based on Neural Networks," *Proc. of 2002 Inter. conf. on Machine Learning and Cybernetics*, Sydney 2002.

Luo Zhong is a Full Professor and a tutor of Doctor, a head of the School of Computer Science and Technology, Wuhan University of Technology, the principal of Graphic & Intelligent System, a judge of Nature & Science Fund. He graduated from Wuhan University in 1982 and achieved Doctor's degree from Wuhan University of Technology in 1995 with specialty of structure. He visited Japan and France as scholar; was awarded many prizes by government and has published a lot of papers in kernel journals, which can be searched partly by EI/SCI/ISTP. His research interests are in intelligent technology, expert system, neural network, software engineering, artificial intelligent, distribute computing, image & graphics and parallel processing.

Scene Dispatch Strategy Based on Nerve Network

Dongmei Yang, Churong Lai, Guisheng Yin and Ganggang Zhang
Computer Science&Technology College, Harbin Engineering University
Harbin, Heilongjiang Province,China
Email: ydm411@sohu.com

ABSTRACT

According to the characteristic of the virtual assembly, Markoo model of variable viewpoint state has been established. The scene dispatch method based on nerve network is put forward owing to the finding of the rule of viewpoint change during the assembly process with the uses of the nerve network. This method is adopted to call in the scene ahead of time that is going to appear in the assembly process. The strategy may enhance the efficiency of the scene dispatch and cause the dispatcher intellectualized, so as to achieve the goal of the real time display scene. This dispatcher strategy may be also applied in such domains of virtual reality as the scene roams.

Keywords: Scene Scheduler, Virtual Assembly, Neural Network, Markov

1. INTRODUCTION

In virtual reality, the scene dispatch is an important constituent of virtual scene management. According to its purpose, the virtual scene management technology can be divided into two kinds: one is taking the object as the unit facing interact; and the other is taking the space as the unit facing performance. The corresponding scene dispatch consists of object-oriented dispatch and spatial dispatch. The scene dispatch chooses a scene by the prismoid for observation, and the scene range of the prismoid for observation depends on the viewpoint state (the viewpoint position and the angle) and its volume. The former scene dispatch is somewhat blind because it rarely uses the semantic information provided by concrete scene. And it affects scene real time display.

Human subjectively decides the changes of viewpoint. Although it has little randomness at a certain time, its changes have certain rules in the specific environment within a long time. Usually people pay attention to a certain part of the scene by some probabilities, therefore when the scene saved in the external memory is move into memory by a certain probability, the one has more probabilities is easier moved.

This phenomenon is more obvious in the process of virtual assembly. Because the operators of the virtual assembly system are technicians with similar knowledge background and same assembly goals, the scene they want to see is usually the same. They need to repeat the whole assembly process or to carry on an exploratory installment for some component while they are performing the virtual assembly. The same scene and the assembly process repeatedly appear provided the semantic information needed by scene dispatching.

The viewpoint change decided subjectively by the human, that has certain randomness in some time, but its change has certain rule in the specific environment within a long time. Usually people pay probability attention to some part of certain scene[2], and the scene which save in the external memory is called into the memory by a certain probability, therefore the more people pay attention the more possible the probability called in.

When carries out the assembly to some components, we can found that the viewer viewpoint information change is stochastic in one time, as a whole, the viewpoint information change may regard as is a Markov process, which has the relatively stable way and relatively stable angle of view in the corresponding position regarding the specific components, also changes by certain probability to the next condition. Because the viewpoint information decide the scene, if these useful information can be used appropriately we can enhance the scene demonstration timeliness.

The neural network has the ability to memory fuzzy information, which may be used to study and memory the information of virtual assembly process. When the training network is stable, we can dispatch the assembly scene through the output information of the network. We establish a Markov decision-making model based on viewpoint change, and find the viewpoint change of state rule of virtual assembly by neural network, and forecast viewpoint change by the output, and carries on the scene dispatch to enhance the demonstration efficiency. This method also may expand to other domain scene dispatch in the virtual reality.

2. MARKOV MODEL BASED ON THE CHANGE OF VIEWPOINT STATE

Markov model based on the change of viewpoint state refers to the condition the viewpoint has achieved, only relies on the condition which locates at present, having nothing to do with the condition which formerly located [3]. Therefore in the virtual assembly, the viewpoint state change may be regarded as a random walk process. Suppose the viewpoint state is expressed as $\{ X(t), t \in T \}$, in which t is the assembly time, it is separate, $X(t)$ is decided by the state of the viewpoint $X(i) = (x, y, z, h, p, r)$ which locates in the t time, the position in which the viewpoint locates is (x, y, z), the angle of view direction is (h, p, r). The viewpoint condition has nothing to do with the outset time, therefore the viewpoint change process is the odd Markov process.

As part of the printing process your document will be photographed. To ensure that this can be done with one camera setting for all papers and to ensure uniformity of appearance for the Proceedings, your paper should conform to the following specifications. If your paper deviates significantly from these specifications, the printer may not be able to include your paper in the Proceedings.

Suppose the viewpoint state space is $S = \{1, 2, 3 .....\}$, and it is limited. The state space may be divided into two ways. Unreachable state, the state that the viewpoint can't arrive at; the other is the reachable the state, the state which the viewpoint can arrive at. The number of the state spaces can be

set, for example assemble space can be divided into 100×100×100 points, and each angle of view can be divided into 360×360×360, in other words, there are 100×100×100×360×360×360 states. The change of the space division granularity changes the precision that regards the special details to decide.

Most of the random phenomenon has a stable average result; therefore the viewpoint transfers into the next state by a stable probability. Each viewpoint state has 12 operations, it means that, when one component of the state of the viewpoint $X(i) = (x, y, z, h, p, r)$ increases an operation unit or reduces an operation unit, the operation unit's size decided by the spatial division granularity and each operation is chosen by certain probability, and the viewpoint state shifts when one operation is chosen. For example, when viewpoint move one unit to X, the viewpoint $X(i) = (x, y, z, h, p, r)$ will turn to $X(j) = (x+1, y, z, h, p, r)$.

One step transition matrix:

$$P = \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & \ldots & \end{array} \\ \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} & \ldots\ldots & P_{1n} \\ P_{21} & P_{22} & P_{23} & P_{24} & \ldots\ldots & P_{2n} \\ P_{31} & P_{32} & P_{33} & P_{34} & \ldots\ldots & P_{14} \\ P_{n1} & P_{n2} & P_{n3} & P_{n4} & \ldots\ldots & P_{nn} \end{pmatrix} \end{array} \begin{array}{c} 1 \\ 2 \\ 3 \\ \end{array}$$

In the matrix $P_{ij} \geq 0$, $\forall i, j \sum_{j} P_{i,j} = 1$, there are only 12 probabilities can not be zero in one row, and the other are all zero, because it is possible that the other states are get in one step. If i and j is reachable, it means that i can get j in limited steps. For example, P_{15}=0,it means state 1 can't reach state 5 in one step, but state 1 may arrive at state 5 through state 3, and its probability is $P_{13} * P_{35}$. $p_{ij}^{(k)}$ means the probability which state i gets state j in k steps. $\lim_{n->\infty} p_{ij}^{(k)} = 0$ means state i can't reach state j.

Using the above probability information provided by the Markov model may forecast the scene condition directly. Every time the specific component is assembled, the corresponding viewpoint starts with the same original state. After the assembly starts, each viewpoint change situation is recorded, the component is repeatedly assembled, calculate the probability of the operation under the specific viewpoint state, then establish the matrix of state transition probability to components, finally carry on the same operation establishment corresponding the matrix of state transition probability to all components. When this components is assembled again, assign out the corresponding components the transition matrix to manage the scene dispatch, namely the viewpoint carries on the state shift according to the most probability

Although this method may carry on the scene dispatch, it has the obvious insufficiency. It needs massively data to obtain the viewpoint state transition probability matrix, and also needs to maintain this matrix for each component; therefore it needs massive computations and storage space. Therefore we proposed a scene dispatch strategy based on the neural network technology in next section.

3. STRUCTURE NEURAL NETWORK

The neural network may save the environment experience knowledge through training [4], the experience knowledge here refers to the change rule of the viewpoint condition, and it saves in weight form in the weight matrix. In fact, training neural network to simulate the Markov process is the process of approaching a complex function; regulating the network weight, enable the function it expresses to output with expectation, so that we may forecast viewpoint condition through the neural network simulation function. We can also simulate this Markov process by multinomial and the transect line, but these methods are not strong enough, and the versatility is not good. Realizing the Markov decision-making process with the neural network can overcome these shortcomings and we can use the BP network to simulate Markov process [5]. Here unifying the characteristic of viewpoint change in the virtual assembly, and using radial direction primary function network to realize the forecast function of the Markov process.

The radial direction primary function network is a kind of front network based on function approximation theory. It will lower the best-fit plane of space mapping to the multi-dimensional space to seek the training data. Radial direction primary functions is superior to BP network in many aspects regardless of approaching ability、classifying ability、study speed and so on. The structure of this network is shown as followed:

Consider instance $\{(x_i, d_i)\}^{N}_{i=1}$ as training sample, vector x_i is the input of the network expressing the current actual condition of viewpoint, d_i is the actual following condition of x_i, $\{(x_i, o_i)\}^{N}_{i=1}$ is the input and output of the network, . .

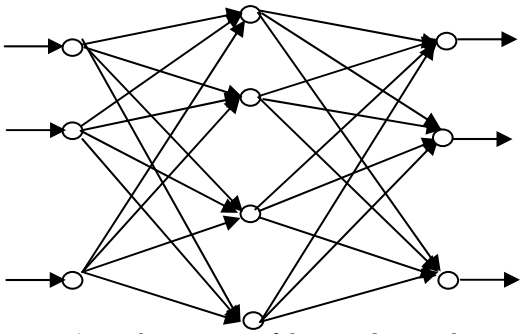


Fig.1. The structure of the neural network

o_i is the output of the network expressing the forecast following condition of x_i, N is the sample number, this kind of network only has one concealed level, w_{ij} is the connection weight between neuron i to neuron j in the concealment level. Taking the Gaussian function as the primary function here : $\phi(x, \sigma) = \exp[-\| x - c_i \|^2 / \sigma^2]$, $\| x - c_i \|^2$ is the distance from X to c_i, c_i, σ is the center and the width of the radial direction primary function respectively and can be determined by K-average value cluster algorithm law[4], that is:

$$C_j = 1 / numb(\theta_j) \sum_{x_j \in \theta_j} X_j \quad (1)$$

$$\sigma = d_m / \sqrt{2M} \quad (2)$$

θ_j is the cluster subset, $numb(\theta_j)$ is the sample number of θ_j, d_m is the maximum range between various centers, M is the thinking.

The training sample collection, suppose an operation of 100 steps can complete some component's assembly, then it experiences 101 conditions (including the original state) altogether and produce 100 training samples $\{(x_i, d_i)\}^{100}_{i=1}$ altogether. The training samples select the central method through the neural network and determine c_i, σ according to sample determination.

The determination of concealed level neuron number, using cut and try method [6] make concealed level include a few neurons first, then increases the number gradually and stop after the network output reaching the precision request, so that the network has the smallest structure.

When carry on the virtual assembly, CPU is at the busy condition, so you must consider the computation cost of the neural network. Use the way of collecting the data in the actual assembly and training the network when separated from the environment to carry on the training and record the corresponding components weight matrix. When the training has been completed, the input and output need extremely little time in using the neural network, so it can meet the needs of the real-time way.

4. ASSEMBLY PROCESS

Accurately indeed settles the next step of viewpoint condition, maybe there is different between viewpoint condition and the forecast viewpoint condition.

Actual scene formation of the aligment:

S_{i-4}	S_{i-3}	S_{i-2}	S_{i-1}	S_i

Forecast view point condition of the aligment:

S_{i+1}	S_{i+2}	S_{i+3}	S_{i+4}	S_{i+5}

S_i is the current condition of the viewpoint state, and S_{i-1} to S_{i-4} are the past condition (real viewpoint state), S_{i+1} to S_{i+5} are the condition following network forecast current Regarded. The volume and the viewpoint condition of the the prismoid for observation decide the spatial region which regarded the prismoid for observation occupies.

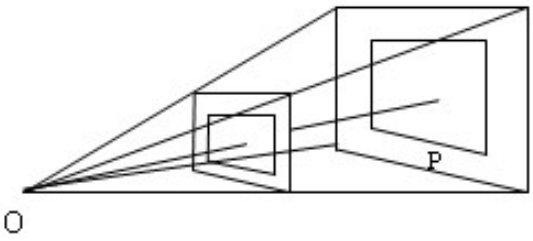


Fig.2. The prismoid for observation

Suppose V_i is the spatial region that the current viewpoint condition decided, V_k is spatial region that decided by the next condition of S_i.

Gathers V_r is a union set spatial regions occupied by the prismoid for observation, which is decided by past viewpoint condition in actual scene formation.

$$V_r = V_{i-4} \cup V_{i-3} \cup V_{i-2} \cup V_{i-1} \quad (3)$$

Gathers V_p is a union set spatial regions occupied by the prismoid for observation, which is decided by forecast viewpoint condition in forecast scene formation.

$$V_p = V_{i+4} \cup V_{i+3} \cup V_{i+2} \cup V_{i+1} \quad (4)$$

If $V_k \in V_p \cup V_r$, it means the scene the accurate forecast needs is already in the memory, simultaneously the neural network forecasts the next condition of S_{i+5}, and enters the team, also S_{i+1} set out.

If $V_k \in V_p \cup V_r$,it means a part of the scene needed is not in the memory, and this part of scene is supposed as $V_s = V_k - V_p \cup V_r$,Needed to call in by now the memory: If the surplus memory is bigger than or equal to the memory needed by V_s, then call it in directly; If the surplus memory is smaller than the memory needed by V_s, then it needs to assign the partial scenes out of the memory which the method to discover in the actual scene formation causes$\| S_k - S_j \|$ Biggest, in which j=i-1, i-2, i-3 i-4，actual current viewpoint condition following actual viewpoint condition. ||.||is norm, then assigns out the scen hypothesized e for $V_k - V_j$ also set out, if the memory is still insufficiently duplicates, repeat the above process till it can seat the scene.

5. CONCLUSIONS

In view of the characteristics of viewpoint information change in assembly, the viewpoint change of state Markov model has established under the hypothesized assembly environment. The viewpoint change of state direction dissemination neural network has been established based on neural network learning capability. Forecast the next step or the next several steps of viewpoint condition information through the output of the net, and carry on the hypothesized assembly scene the dispatch with the information of the prismoid for observation scope. And with the fault-tolerant technology, it made the neural output result.

Fuzziness and the scene dispatch precise disposition contradictory better. Enhance the timeliness of the scene dispatch simultaneously, it can be also used for scene dispatch in other domains in virtual reality.

REFERENCES

[1] Baichang Luo, Ming Chang, "Face Virtual Environment Scene Management Essential Technology and Its Realization Research," *Journal of System Simulation, vol. 15, no. 6,* 2003.

[2] Duwu Cui, Zhurong Wang, "The Research And Realization of Dispatch Algorithm In Virtual Roams System," *Computer Engineering, vol. 28, no.12,* 2002.

[3] Yongcai Mao, Qiying Hu, *Stochastic process*. Xi'an Electron Scientific And Technical University Publishing House,2002.

[4] Simon Haykin, *Neural Network*, Mechanical industry publishing house, 2000.

[5] Dai Kui, Hu Shouren, "The nerve network reliability design Based on separated Markov Model," *Computer Engineering and science*, 1999.

[6] Yin Guisheng, Liu Qun, Zhang Jianpei, Liu Jie, Liu Daxin, "Petri Based Analysis Method for Active Database Rules," *IEEE Intl. Conf. on SMC, vol.4, no.2*, 1996,pp.858-862

[7] J. S. Dong, J. Colton, and L. Zucconi, "A Formal object approach to real-time specification," In *the Asia-Pacific Software Engineering Conference Seoul, Korea, December*, IEEE Computer Society,2003.

Research on the Regulated Morphological Method and its Application Based on Neural Network

Qisheng Yan[1]
School of Mathematics & Information Science, East China Institute of Technology
Fuzhou[2], JiangXi[3] 344000, China
Email:yanqs93@126.com

ABSTRACT

The basic concepts of regulated morphological operations have been introduced firstly, In order to enhance the robustness of morphological image processing as well as the performance in the anti-disturbance, a novel implementing method based on neural network (ANN) has been presented. This Method has been applied to binary image filtering and edge-detection. The experimental results demonstrate that the noise can be nearly removed by using the new method and the detail of original image can be kept clearly with the clear edge, thus its performance is better than the classical morphological filter. In addition, the method has the feature of flexibility than classical morphological operations.

Keywords: Regulated Morphological operations, Mathematical morphology, Neural networks, Filtering, Edge-detection

1. INTRODUCTION

Mathematical morphology, which is based on set-theoretic concept, provides an efficient tool to image processing, and analysis [1-3].It is widely adopted in computer vision, signal processing, image analysis, pattern recognition, and it includes almost all the concerned contents of the image processing, such as nonlinear filtering, texture analysis, biological material analysis, edge detection, feature extraction, image compression, image segmentation and face recognition etc. Since the 90's of 20th century, the method of combination of classical mathematical morphology and soft computational method and wavelet and fractal theories has been widely applied to computer vision and pattern recognition.

The classical filter based on the standard morphology has the better performance for denoising, at the same time it vagues the edge information of image, the robustness of morphological image processing as well as the performance in the anti-disturbance which is in the need of development.
Since the efficiency of the morphological filter is mainly up to the following two factors: One is the definition of basic morphological operators (dilation and erosion) and the structuring element. The other is the selection of structuring element and the construction of composite operators. To the former, we can develop it in two ways: one is to divide the structure element into two parts: the core, the pixels participate with weights greater than one, and the soft boundary, the pixels participate with weights equal to one, then get the soft morphological operators [4]. The other is to define a class of morphological operations such as regulated morphological operations by extending the fitting interpretation of the ordinary morphological operations, which have a controllable strictness, and so they are less sensitive to noise and small intrusions or protrusions on the boundaries of shapes[5].In addition, due to the complexity of image information and the strong relevance among them, there are probably some incompletion and inaccuracy under various situations during the process, so the better processing performance may be obtained by applying fuzzy set theory to the image processing and understanding in some situation. In Ref. [6], a fuzzy morphological method with one restricted parameter (r-MM) is presented. In this paper, Neural network implementation of regulated morphological operations have been discussed. Experiment results show that the method of combination of regulated morphological operations with neural networks can obtain a good effect in filtering and edge-detection for binary images.
In what follows, X will denote an image and it will present the set of black pixels as in the binary case. The cardinality of a set S is denoted by $|S|$. we will call S a symmetric set if $-S = S$ .The translation of a binary image X by s, $\{x+s, x \in X\}$ is denoted by $X_{(s)}$.

2. CLASS MORPHOLOGICAL OPERATION AND REGULATED MORPHOLOGICAL OPERATION

2.1 Dilation operation

The dilation operation may be interpreted in various ways. In particular, the dilation of X by S (S is a symmetric) may be obtained as the union of all the possible shifts for which the shifted S intersects X .That is

$$\rho_S(X) = \{x \mid X \cap S_{(x)} \neq \varnothing\} \qquad (1)$$

By using the fitting interpretation of dilation (1), the morphological dilation of X by S can be extended by combining the size of the intersection into the dilation process. In that sense, a given shift is included in the dilation of X only if the intersection between X and the shifted S is big enough. The obtained advantage of the regulated dilation is the prevention of excessive dilation caused by small intersections with the object set[5].

Definition 1. The regulated dilation operator $\tilde{\rho}()$ of X by S is defined by:

$$\tilde{\rho}(): \quad \tilde{\rho}_{r,S}(X) = \{x : |S_{(x)} \cap X| \geq r\}$$

where $r \leq |S_{(x)} \cap X|$.

2.2 Erosion Operation

It can be know that dilation and erosion are dual, so that the morphological erosion of X by S (S is a symmetric) can be obtained by dilating the complement of X with S, and then taking the complement of the result. That is

$$\varepsilon_S(X) = (\rho_S(X^c))^c$$

where X^c denotes the complement of X defined by: $X^c \equiv \{x | x \notin X\}$ .The erosion operation may be interpreted in various ways. In particular, one interpretation is: $\varepsilon_S(X) = \{x \mid X^c \cap S_{(x)} = \varnothing\}$

So regulated erosion operator can be defined as following[5]:

Definition 2. The regulated dilation operator $\tilde{\varepsilon}()$ of X by S is defined by:

$$\tilde{\varepsilon}() : \tilde{\varepsilon}_{r,S}(X) = \{x : |S_{(x)} \cap X^c| < r\}, \quad r \in [1, |S|].$$

Considering every pixel of binary image, we can interpret classical morphological dilation and erosion operators as following in another ways:

$$\varepsilon_S(X)(x,y) = \begin{cases} 1, & if\ |X \cap S_{(x,y)}| = |S| \\ 0, & otherwise \end{cases}$$

$$\rho_S(X)(x,y) = \begin{cases} 1, & if\ |X \cap S_{(x,y)}| \geq 1 \\ 0, & otherwise \end{cases}$$

where $X(x,y)$ denotes the value (0 or 1) of pixel in coordinates (x,y), So we can get that

$$\tilde{\rho}_{r,S}(X)(x,y) = \begin{cases} 1, & if\ |X \cap S_{(x,y)}| \geq r \\ 0, & otherwise \end{cases} \qquad (2)$$

It should be noted that this formula result in the classical erosion and dilation respectively when r is $|S|$ and 1 respectively.

3. THE REGULATED MORPHOLOGICAL METHOD BASED ON ANN

In recent years, the parallel computing performance and non linear mapping and adaptive ability of ANN have got well known along with the in-depth research of neural networks. neural network models have been widely employed in lots of fields. In this paper, a implementing method based on neural network will be discussed.

Let

$$\tilde{M} = \{x \in I^2 \mid |X \cap S_{(x)}| \geq r\}$$

we can get

$$\tilde{M} = \left\{ x \in I^2 \mid \frac{|X \cap S_{(x)}|}{r} \geq 1 \right\}$$

$$= \left\{ x \in I^2 \mid \frac{\sum_{y \in X \cap S_{(x)}} \mu_{X \cap S_{(x)}}(y)}{r} \geq 1 \right\}$$

$$= \left\{ x \in I^2 \mid \sum_{y \in X \cap S_{(x)}} \frac{\mu_{X \cap S_{(x)}}(y)}{r} \geq 1 \right\}$$

that is

$$\tilde{M} = \left\{ x \in I^2 \mid \sum_{y \in S_{(x)}} \frac{\mu_{X \cap S_{(x)}}(y)}{r} \geq 1 \right\} \qquad (3)$$

where $\tilde{M}$ denotes a morphological operation(dilation or erosion), I^2 denotes the integer space of two-dimension, $\mu_{X \cap S_{(x)}}(y)$ denotes the membership function of y belongs to $X \cap S_{(x)}$, and we can get that $\mu_{X \cap S_{(x)}}(y) \in \{0,1\}$ for binary images. r is a constraint parameter and $r \in \{1, \cdots, |S|\}$ .Now we regard $1/r_i$ as the weight ω_i of neural network and regard $\mu_{X \cap S_{(x)}}(y)$ and $y \in S_{(x)}$ as the input I_i （$i = 1, 2, \cdots, |S|$） of neural network, and obviously we can get that

$$\omega_i \in \left\{ 1/|S|, 1/(|S|-1), \cdots, 1 \right\},$$

and then $\tilde{M}$ can be denotes as

$$\tilde{M} = g(\sum_i^{|S|} \omega_i I_i - 1)$$

where $g(x)$ is a threshold function.

This is a typical expressing way for neural network, and $\tilde{M}$ can be implement by using a simple perception model as fig.1.

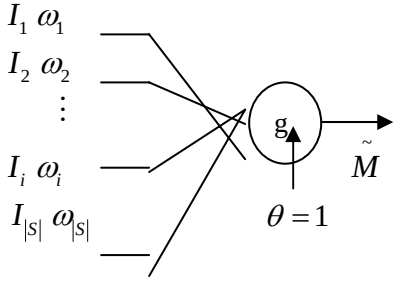


Fig.1. Simple perception model

For binary image, $g(\bullet)$ is defined by

$$g(u) = g(\sum_i^{|S|} \omega_i I_i - 1) = \begin{cases} 1 & u \geq 0 \\ 0 & u < 0 \end{cases}$$

It is clearly that ω_i is $1/|S|$ and 1 when r is $|S|$ and 1 respectively, and its corresponding morphological operation is classical erosion and dilation respectively. But we can obtain a operation result between classical erosion and classical dilation.

4. EXPERIMENTAL RESULTS

In order to demonstrate the performance of the regulated morphological method based on ANN, we compared it with the classical mathematical morphology in noisy image processing. Fig.2. presents an example of morphological processing of a noisy image by using our method and the classical morphological operations respectively. The

structuring element used in these operations is a 3×3 flat structuring element with the origin at its center.

(a) original image X

(b) X corrupted with gaussian noise (0, 0.05)

(c) erosion result using classical morphological method

(d) dilation result using classical morphological method

(e) filtering result using regulated dilation based on ANN
r=4

Fig.2. Result of computer simulation for filtering

Fig.3. presents an example of edge-detection of a noisy image by using our method.
If the value of r can be at a certain range not a determined value. we can let

$$r = r_0 + \Delta r$$

and then $\tilde{M}$ can be modified into

$$\tilde{M} = \left\{ x \in I^2 \mid r_0 \le \sum_{y \in X \cap S_{(x)}} \mu_{S_{(x)}}(y) \le r_0 + \Delta r \right\}$$

selecting proper r_0 and Δr, we can obtain the edge of binary image. where the structuring element used in the operation is a 3×3 flat structuring element with the origin at its center.

(a) original image X

(b) X corrupted with gaussian noise (0, 0.05)

(c) edge-detection result using our method
r_0 =4, Δr =2

Fig.3. Result of edge-detection for noising image

From the above experiment we can observe that the noise can be nearly removed by using our method and the detail of original image can be kept clearly with the clear edge.

5. CONCLUSIONS

In this paper, we studied a regulated morphological method based on ANN, and tried to apply the method in binary image filtering with great experimental success, it is to some degree development of the classical mathematical morphological method. But how to apply this method widely in the actual image like grey, colorful image etc and wider fields in image processing is our next step works.

REFERENCES

[1] Etienne Decencie're, Marcotegui B, Meyer F. "Content-dependent image sampling using mathematical morphology: Application to texture mapping"[J].*Signal Processing: Image Communication*, 2001,16:567-584
[2] JSerra.Image *Analysis and Mathematical Morphology* [M]. Academic Press，London，1988.
[3] E R Dougherty. *Mathematical Morphology In Image*

Processing[M].Marcel Dekker，1993.

[4] Koskinen L. SoftMorphological Filter. Proc. “Proceedings of SPIE-The International Society for Optical Engineering,” 1991, 1568（1）: 262-270.

[5] Gady Agam, Its’hak Dinstein. “Regulated morphological operations,” *Pattern Recognition*, Vol.32, 1999, 947-971.

[6] Q.S. Yan, “A New Denosing Algorithm Based on FuzzyMathematical Morphological Operations with One Parameter,” *the fifth International Conference on Distributed Computing and Applications for Business*, Engineering and Sciences, 2006,vol.2:755-758

The RBF Neural Network Prediction for Futures Contract Price

Mengdong Wang, Wenjing Chen
School of Sciences, Wuhan University of Technology,
Wuhan 430070, China
Email: E8556@126.com

ABSTRACT

In this paper, RBF Neural Network is used to forecast futures prices and trend. Based on RBF Neural Network Theory, we focus on the forecast of London Copper by MATLAB Software. The results show that RBF Neural Network can be well used in the prediction of the futures contract prices.

Keywords: RBF Neural Network, Nonlinear Time Series Prediction, MATLAB Simulation

1. INTRODUCTION

Futures markets touch the hearts of millions of investors, since its birth date. Futures prices affected by many factors, such as supply and demand, monetary, financial market changes economic cycle changes, political events, the government policy measurements human action, psychology and so on [1]. However there are no definite rules to describe these factors. People used in the futures market analysis include traditional statistical method, which mainly based on people's experience to sum up the chart state, indicators formula to describe the market changes. In recent years, with the development of artificial intelligence science, a new artificial intelligence method has been used in futures prices forecast. In the artificial intelligence technology, the neural network prediction method is commonly used.

Neural network, has a strong ability of self-study and error revision, theoretically it was proved to approach to any nonlinear system [2]. In the neural network algorithm, the BP algorithm application is widespread, while as BP algorithm's weight-value adjustment is the negative gradient method. It has a slow convergence and easy to be trapped in a local minimum value, thereby affects the accuracy of forecasts and reliability. In this paper, we use approximation, Classification and learning speed which are better than BP network RBF neural network model to predict futures prices. Simulation results show that the model can effectively predict on futures prices for short-term forecasts.

2. RBF NETWORK'S STRUCTURE AND ALGORITHM

The RBF Neural Network is the three-tier network. It constitutes input layer, hidden layer and output layer. As futures price is a one-dimensional time series, so the output layer is only one element. The topology of the RBF Neural Network is shown in Fig1.

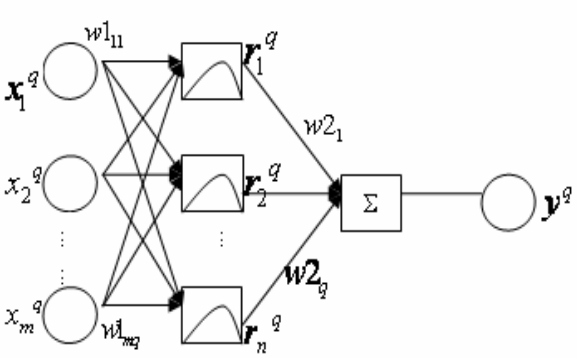


Fig.1. The topology of the RBF Neural Network.

Fig. 1 shows the structure of m-n-1 RBF network, the networks with input m, n implicits and one output. Where let denote the input vector be $x^q = (x_1^q, x_2^q, \cdots x_m^q)^T \in R^n$; $w1 \in R^{m \times n}$ denote the input power matrix, $r_i^q(*)$ denote the hidden node activation function; $w2 \in R^{n \times 1}$ denote the output power vector, y^q denote the network output. Σ in the output layer express that output layer neurons use linear-activation function . The RBF network's most notable feature is that people use the distance function as the hidden node-function and use RBF function as the activation function. Generally Gaussian function is the most classical function in the RBF network.

The information processing of REF neural network can be divided into the implementation phase and learning phase. Implementation phase refers to the neural network deals with the input information and produces output in the process.
The input of the hidden layer neurons is as follows:

$$s_i^q = \| w1_i - x^q \| \times b1_i \quad (1)$$

Let $\| * \|$ denote the Continental Norm; $w1_i$ is the weight vector, which connected with the i-th value of input layer and the hidden layer neurons. Let x^q denote the Input vector; $b1_i$ denote the threshold of the value of the hidden layer, which can adjust the sensitivity of the function.
Gaussion function is used as an activation function. the output of the i-th hidden layer is as follow:

$$r_i^q = \exp(-(\| w1_i - x^q \| \times b1_i)^2) \quad (2)$$

In the neural network toolbox of the MATLAB software, the relationship between $b1_i$ and k_i is that: $b1_i = 0.8326 / k_i$ .let k_i denote the Constant expansion of the i-th hidden layer. At this point the input of the hidden layer neuron is as follows:

$$R_i^q = \exp\left[-0.8326^2 \times \left(\frac{\| w1_i - x^q \|}{k_i}\right)^2\right] \quad (3)$$

The value of the output layer is the weighted sum of the values, which are from the hidden layer neurons.

$$y^q = \sum_{i=1}^{n} R_i^q \times w2_i \quad (4)$$

Generally, the Learning stage of the neural network is self-improvement stage. The RBF network uses error correction learning process. Let the center value of the i-th hidden layer be k_i . If we determined k_i , the formula (4) is a linear-equations. hence, the problem of calculating the weight vector $w2$ is becoming a linear-optimization problem. In this paper, the recursion of least squares method to solve this problem.

Objective Function:

$$J(t) = \sum_{p=1}^{n} E_p(t) = \frac{1}{2}\sum_{p=1}^{n} \Lambda(p)(d^q - y^q) \quad (5)$$

Let $\Lambda(p) = \lambda^{n-p}$ denote the weighted factor. Le d^q tdenote the actual output value, and let the calculation of the output samples be y^q . So the value, which makes $J(t)$ achieve to minimum, is the value of the demand. We can have the result from the equation, that is $\frac{\partial J(t)}{\partial w2} = 0$.

3. THE RBF NEURAL NETWORK PREDICTION FOR FUTURES CONTRACT PRICE

In the futures market, the futures price indices measure is including opened, the dollar, the highest price, the lowest prices, volume and so on. In this paper London-cop futures dollar as a study of data samples and forecasting. Here we selected London-cop futures price from April 3.2006 to March 26.2007, between 250 trading days data to analyze the futures price. The data processing is including the following three stages.

3.1 Normalize the Data in Minimax Value Method

Suppose the time sequence $x = \{x_i \mid x_i \in R, i = 1, 2, \cdots L\}$, whose length is $N + M$ with overlaps. The specific method as follows:

Table 1. The specific method of dealing with data

Input data（N dimension）	output（M dimension）
$x_1 \cdots x_N$	$x_{N+1} \cdots x_{N+M}$
$x_2 \cdots x_{N+1}$	$x_{N+2} \cdots x_{N+M+1}$
…	…
$x_N \cdots x_{N+K-1}$	$x_{N+K} \cdots x_{N+M+K-1}$

Taking into account that the minimax value method can normalize all the data to the data (between 0-1), and this can facilitate the mathematical procession. So the importation of samples has been initialized by the minimax value method. Specific algorithm: calculate the maximum and minimum of the original data in this period. Let denote the maximum data be Max and the minimum data be Min .The corresponding value of x_i will be $x_i' = \frac{x_i - Min}{Max - Min}$ [5].

3.2 The RBF Network Training and Optimization with MATLAB Software

Here we set every 10 days as a cycle, the 10-day future prices data as the input vector, and then we get the future price on the forecasting current day as the output data. Thus, the number of neurons on input layer is N=10, on output layer is M=1. Suppose the number of neurons on middle layer is 50, we use network to create codes:

Spread =10;

Net =newrbe (P,T,spread);

Where, spread denotes the RBF distribution, P and T denote the input and output vector in the training sample respectively and newrbe expresses the order to create an exact RBF. The error of this net is 0.

We use the first 10 samples as a training sample and the next 6 samples are used as the test samples. The test code is that: Y=sim(net,P_test); P_test is the vector of the testing samples.

3.3 The Result of the Analysis

The following is the comparison between the forecast prices and the actual value on London cop future price.

Table 2. The result of the analysis

date	2007/1/24	2007/1/25	2007/1/26	2007/1/26	2007/1/30	2007/1/31
Actual Value	0.3823077	0.5692308	0.5	0.1576923	0.2769231	0.3923077
Predicted Value	0.3392552	0.4318182	0.4555338	0.131	0.2244719	0.3918
Absolute Error	0.0430525	0.1374125	0.0444662	0.0266923	0.0524512	0.0005077
Relative Error	0.1126121	0.2414004	0.0889323	0.1692683	0.1894071	0.0012941

From the results we can see that RBP Neural Network futures prices on the short-term effect are better. The average absolute error in the forecast is no more than 0.06. And forecast better directional price movements. From April 3, 2006 to 2007 to March 26, the 271 days of data can be used at forecasting and the results are as follows:

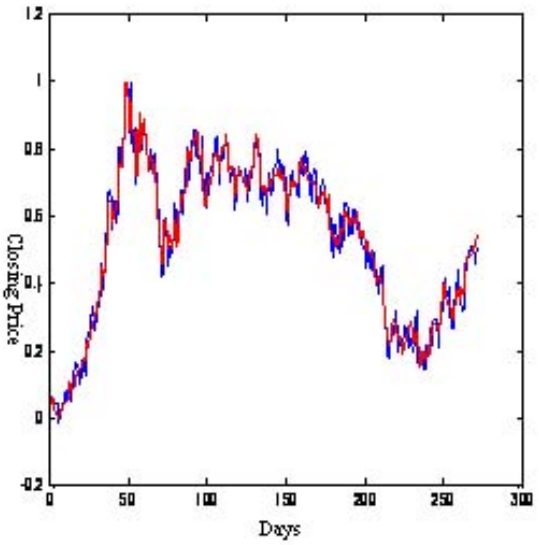


Fig.2. The comparison between Actual Value and Predicted Value during April 3.2006 to March 26.2007

4. CONCLUSIONS

Experimental results show the RBF Neural Network with faster operation's speed and the best approximation properties will be applied to forecast futures price, the actual forecasts and actual data model in achieving obtain better results. In this paper, data are used as a group of relatively stable data, which is derived from future market with normal operation. There are a lot of external factors influence futures price. How to improve the RBF network so that the network has a better predictive capability, we still need further discussion.

REFERENCES

[1] Cheng QiZhi, Gao HongGui, *Futures and the Futures Market,*Wuhan Industrial University Press 1998.299-307.in english

[2] Meng XiangZe, etc., "Multi- Models Coordination stock Market Forecast Based on the Fuzzy Nerve Network", *Papers Collection of Chinese control Conference*, 1997. in english

[3] *Fei Thinking Technology Products R & D ,Center, Neural Network Theory and MATLAB7 Impl ementation*, Electronics Industry Publishing House, Nov 7,2005. in english

[4] Zhu Da Qi, Shi Hui, *Artificial Neural Network Theory and Application*, Scientific publishing house. in english

[5] Cao Qing, Gao Feng, "Stock Market Forecast Based on Nerve Network", *10th Session of nationacademic Annual meeting collection of China Artificial Intelligence Academic society(2003)*, China Artificial Intelligence Academic Society, Beijing Posts and Telecommunications Publishing house

Life Distribution Recognition Using Neural Network

Shang Gao
School of Electronics and Information, Jiangsu University of Science and Technology
Zhenjiang Jiangsu 212003, China
Email:gao_shang@hotmail.com

ABSTRACT

In general, we describe three different methods to select an appropriate distribution form: histogram, probability plots, hypothesis test. The life distribution is recognized by neural network method. The relationship among life distribution with life data is described through threshold and weight of neural networks. The method is convenient to be used. An example is presented, and the results are valid and satisfied.

Keywords: Neural Network, Back-Propagation Algorithm, Recognition

1. INTRODUCTION

In analyzing random data, we must select a probability distribution. In general, we describe three different methods to select an appropriate distribution form: histogram, probability plots, hypothesis test. The formers are direct and rougher, but the latter should estimate parameter first and results depend on the level. In this paper, the life distribution is recognized by neural network method according to life data.

2. DISTRIBUTION RECOGNITION PRINCIPLE USING NEURAL NETWORK

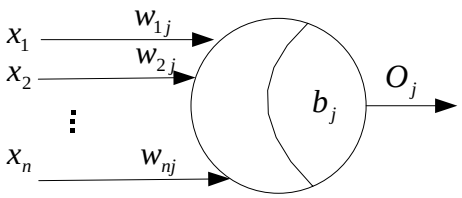


Fig.1. The neuron

The main feature of neural network is that it can learn the internal characteristics of a system by analyzing datasets[1][2]. A neural network consists of simple processing units and each of the processing units has natural inclination for storing experimental knowledge and making it available for use. These simple processing units, called neurons or perceptrons, form distributed network. An artificial neural network is an abstract simulation of a real nervous system that contains a collection of neuron units communication with each other via axon connections. Due to its self-organizing and adaptive nature, The model potentially offers a new parallel processing paradigm that could be more robust and user-friendly than the traditional approaches. As in nature, the network function is determined largely by the connections between elements. We can train a neural network to perform a particular function by adjusting the values of the connections (weights) between elements.

A neuron is a processing unit, which has n inputs and m outputs. $x_1, x_2, \cdots, x_n$ are outputs of previous layers. w_{ij} is the weight by which neuron i contribute to neuron $j \cdot b_j$ is the threshold of neuron j .The net input net_j is defined by

$$net_j = \sum_{i=1}^{n} x_i w_{ij} - b_j \quad (1)$$

O_j is the output of the neuron j .Then $O_j = f(net_j) \cdot f$ is a transfer function, which takes the argument input and produces the output. The transfer function is very often a sigmoid function, in part because it is differentiable. The sigmoid transfer function is

$$f(net) = \frac{1}{1+e^{-net}} \quad (2)$$

The back-propagation network represents one of the most classical examples of an ANN, being also one of the most simple in terms of the overall design. The network is a straight feedforward network: each neuron receives as input the outputs of all neurons from the previous layer. We adopt a three-layer back-propagation network. The pretreatment life data are fed to the inputs. The output of network is life distribution. The network has some hidden. The objective is to train the weights and the thresholds, so as to minimize the least-squares-error between the teacher and the actual response.

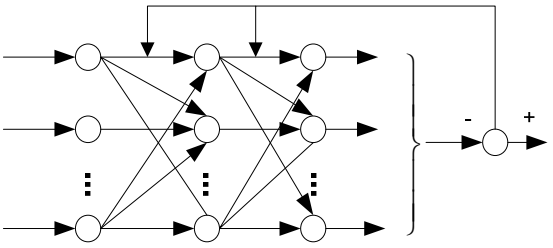


Fig.2. A three-layer Back-propagation network

3. APPROACH DESCRIPTION

3.1 Inputs and Outputs

For the sake of explain the method, we suppose that life data is likely to exponential, normal, lognormal, weibull, or other distribution. Table 1 gives some sample formula[3].

Table 1. Sample formula of several typical distributing

Distributing	Sample formula
Exponential	$-\frac{1}{\lambda}\ln\eta$
Standard normal	$t_{01} = \sqrt{-2\ln\eta_1}\cos 2\pi\eta_2$
	$t_{01} = \sqrt{-2\ln\eta_1}\sin 2\pi\eta_2$
Normal	$t_{01} \cdot \sigma + \mu$
Lognormal	$e^{t_{01}\cdot\sigma+\mu}$
Weibull	$\frac{1}{\lambda}(-\ln\eta)^{1/\alpha}$

Where η, η_1, $\eta_2 \sim U[0,1]$

First we use the sample formula of table 1 to generate N exponential random variables $t_1, t_2, \cdots, t_N$ (where $t_i = -\frac{1}{\lambda}\ln \eta_i$, $\eta_i \sim U[0,1]$, $i = 1,2,\cdots,N$).we divide the $[t_{\min}, t_{\max}]$ into m adjacent intervals. Then we tally f_j (number of t_i in the j th interval for $j = 1,2,\cdots,m$). Note that $x_j = f_j / N$ for $j = 1,2,\cdots,m$. $x_1, x_2, \cdots, x_n$ are inputs of network. Neural network has 5 outputs. For the exponential, the teacher values are (1,0,0,0,0).

Again, We use the sample formula of table 1 to generate N U[0,1] the other distribution random variables $t_1, t_2, \cdots, t_N$ and calculate $x_1, x_2, \cdots, x_m$ respectively which are inputs of network. For the Normal, the teacher values are (0,1,0,0,0). For the lognormal, the teacher values are (0,0,1,0,0). For the weibull, the teacher values are (0,0,0,1,0). For the others, the teacher values are (1,0,0,0,0).

3.2 Numerical Example

We first generate $N = 1000$ exponential random variables with parameter $\lambda = 0.3$, and then divide the $[t_{\min}, t_{\max}]$ into $m = 10$ adjacent intervals. From these data We get $(x_1, x_2, \cdots, x_{10})$ =(0.578,0.241,0.096,0.039,0.020,0.030, 0.001,0.001,0.001). Similarly, we generate 8 samples. Table 2 gives the simulation results. The ANN was trained with the following parameters: learning parameter=0.5, momentum=0.2, error=0.00001. Table 3 gives the trained results.

Similarly, we generate 8 random variables, which are inputs of trained network. The actual output of network can be calculated by using these weights and the thresholds. According to maximal membership principle, we can select a probability distribution. Table 4 gives the results of recognition. the results are very valid and satisfied.

Table 2. Inputs and outputs of network

No.	Distributing	Parameter	Inputs
1	Exponential	$\lambda = 0.3$	（0.578,0.241,0.096,0.039,0.020,0.020,0.003,0.001,0.001,0.001）
2	Exponential	$\lambda = 0.2$	（0.645,0.216,0.089,0.031,0.010,0.006,0.002,0,0,0.001）
3	Normal	$\mu = 5, \sigma = 2$	（0.002,0.011,0.058,0.144,0.202,0.254,0.214,0.081,0.028,0.006）
4	Normal	$\mu = 4, \sigma = 1$	（0.003,0.010,0.051,0.127,0.231,0.278,0.172,0.086,0.035,0.007）
5	Lognormal	$\mu = 4, \sigma = 1$	（0.855,0.108,0.023,0.011,0.001,0,0,0.001,0,0.001）
6	Lognormal	$\mu = 3, \sigma = 1$	（0.765,0.161,0.040,0.013,0.006,0.002,0.007,0.002,0.003,0.001）
7	Weibull	$\lambda = 0.1, \alpha = 2$	（0.096,0.179,0.209,0.204,0.135,0.092,0.048,0.024,0.008,0.005）
8	Weibull	$\lambda = 0.2, \alpha = 3$	（0.033,0.105,0.216,0.253,0.188,0.131,0.049,0.023,0.001,0.001）

Table 3. Results of network

No.	Distributing	Parameter	Teacher values	Outputs of network
1	Exponential	$\lambda = 0.3$	(1,0,0,0,0)	（0.996962, 0.000002, 0.000767, 0.005847, 0.001047）
2	Exponential	$\lambda = 0.2$	(1,0,0,0,0)	（0.988816, 0.000005, 0.010895, 0.000733, 0.000934）
3	Normal	$\mu = 5, \sigma = 2$	(0,1,0,0,0)	（0.000000, 0.994372, 0.003255, 0.004509, 0.000719）
4	Normal	$\mu = 4, \sigma = 1$	(0,1,0,0,0)	（0.000000, 0.995364, 0.004287, 0.003620, 0.000709）
5	Lognormal	$\mu = 4, \sigma = 1$	(0,0,1,0,0)	（0.000514, 0.004290, 0.999355, 0.000000, 0.000403）
6	Lognormal	$\mu = 3, \sigma = 1$	(0,0,1,0,0)	（0.010087, 0.000762, 0.988490, 0.000001, 0.000483）
7	Weibull	$\lambda = 0.1, \alpha = 2$	(0,0,0,1,0)	（0.005483, 0.001880, 0.000000, 0.993876, 0.001093）
8	Weibull	$\lambda = 0.2, \alpha = 3$	(0,0,0,1,0)	（0.001573, 0.006183, 0.000000, 0.995098, 0.001332）

Table 4. Results of recognition

No.	Distributing	Parameter	Outputs of network	Results of recognition
1	Exponential	$\lambda = 0.4$	（0.997569, 0.000002, 0.000130, 0.022564, 0.001039）	Exponential
2	Exponential	$\lambda = 0.5$	（0.987113, 0.000005, 0.011182, 0.000721, 0.000925）	Exponential
3	Normal	$\mu = 5, \sigma = 0.6$	（0.000000, 0.994168, 0.003163, 0.004621, 0.000714）	Normal
4	Normal	$\mu = -5, \sigma = 2$	（0.000000, 0.966790, 0.000267, 0.031285, 0.000809）	Normal

5	Lognormal	$\mu = 2, \sigma = 1$	（0.000331, 0.005852, 0.999574, 0.000000, 0.000403）	Lognormal
6	Lognormal	$\mu = 3, \sigma = 2$	（0.000169, 0.011197, 0.999791, 0.000000, 0.000436）	Lognormal
7	Weibull	$\lambda = 0.3, \alpha = 3$	（0.000256, 0.026530, 0.000000, 0.987927, 0.001484）	Weibull
8	Weibull	$\lambda = 0.2, \alpha = 2$	（0.002676, 0.003858, 0.000000, 0.993913, 0.001236）	Weibull

4. CONCLUSIONS

Neural networks have become a very popular field of research in cognitive science, computer science, signal processing, optics, and physics. It provides a new approach that the life distribution is recognized by neural network method.

REFERENCES

[1] S.Y. Kung, *Digital Neural Networks*. PTR Prentice-Hall.Inc,1993.

[2] S. Singh , A. Amin," Neural network recognition and analysis of hand-printed characters," *in Proc. IEEE International Joint Conference on Neural Networks IJCNN'98, 1998 IEEE World Congress on Computational Intelligence*, Anchorage, Alaska, vol. 3, May 4-9, 1998, pp.1743-1747.

[3] E.E.Lewis, *Introduction to Reliability Engineering*. John Wiley&Sons,Inc,1987

Shang Gao, male, the Han nationality, master, he now works in school of electronics and information, Jiangsu University of Science and Technology. He is an associate professor and He is engage mainly in systems engineering.

Realization and Application Research of BP Neural Network Based on MATLAB

Jie Chen, Bin Xue
School of Electrical and Information Engineering, Wuhan Institute of Technology,
Wuhan 430073, China
Email:ch58j@163.com

ABSTRACT

This paper simply depicts knowledge related to BP network and the algorithm first, then introduces BP tool functions supplied by MATLAB for BP neural network research and how to program within the functions; finally explains the advantages supplied by BP tool functions for BP neural network research with BP neural application in pattern identification and curve imitation.

Keywords: Matlab, BP, Pattern Identification, Curve Imitation, Neural Tool Function

1. INTRODUCTION

In all kinds of network studied today, BP network, which depends on simple structure、strong operation-ability、imitation of every nonlinear relation between input and output, is widely applied in the fields such as function approximation、pattern identification、classification and data compress、image process、system control and so on. Actually, it's to modify weight coefficient ,according to negative grads direction of error function, to make error decrease. Despite wide use of BP network, it will need plenty of data calculation in practice problems. To solve the conflict between data calculation and computer simulation, American Mathworks corporation put forwards the software of MATLAB. The network tool box in MATLAB is a kind of typical network tool function ,based on the theory of network, constructed by MATLAB language, which give much convenience in BP network application research.

2. BP NEURAL NETWORK AND ALGORITHM

BP neural network is a kind of typical forward network, composed of input layer、hidden layer and output layer. Full interconnect form is among the layers(that is, connection between each unit in the former layer and each unit in the next layer). And disconnect form between two neural units of the same layer. The excitation function of every network unit is sigmoid function. Although BP network transmits directly, information transmission is bidirectional. Its structure is as Fig1:

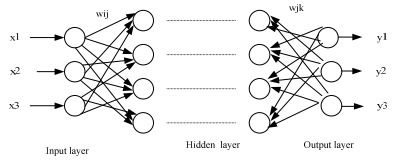


Fig.1. BP Neural Network Structure

After network is decided, BP network studies and modifies the connecting weight and threshold value among neural units, according to the input and output of input example, to make network achieve presented mapping relation between input and output. In terms of it, standard BP study process is divided into two stages: information positive transmission and error reverse transmission[1].

2.1 Information Positive Transmission:
input information, from input layer and processed by hidden layer, is transmitted to output layer.
① input layer: input value is every branch value of the example, output value of input layer is equal to the branch value of the example generally.
② hidden layer: hidden layer has single layer or multilayer. To node j ,its input value x_j is the sum, weightingly adding the output value y_i of every node in the former layer:

$$x_j = \sum_i w_{ij} y_i \tag{1}$$

its output value is:

$$y_j = f_s(x_j) \tag{2}$$

$f_s(*)$ is excitation function, using sigmoid function generally:

$$f_s(x_j) = \frac{1}{1+e^{-(x_j-\theta_j)}} \tag{3}$$

θ_j is the threshold value of node j ,
and $f'(x) = f(x)[1-f(x)]$.
③ output layer: to node k , its input x_k and output y_k are respectively:

$$x_k = \sum w_{jk} y_j \tag{4}$$

$$y_k = f(x_k) \tag{5}$$

Linear functions is usually used in output layers.

2.2 Error back propagation[2]
when the real output value from neural network isn't equal to the expecting value, error e will be gotten. Use the negative gradient descent way to make connecting weigh return following the former connecting access and have error function decrease by modifying the weigh of each layer. Among them, error function generally chooses the LMS error estimator to calculate error.
Suppose the real output from the network is y_{pk} and expecting output is t_{pk} , so mean-square error function E_p is:

$$E_p = \frac{1}{2}\sum_k (t_{pk} - y_{pk})^2 \tag{6}$$

among that, k denotes the k unit of the output. p denotes the p input example.

To all the learning example, the system mean-error is:

$$E = \frac{1}{2P}\sum_{P}\sum_{k}(t_{pk} - y_{pk})^2 \quad (7)$$

Using the steepest descent backpropagation to modify weigh:

① weigh regulation between output layer and hidden layer:

$$w_{jk}(t+1) = w_{jk}(t) + \Delta w_{jk} \quad (8)$$

among that,

$$\Delta w_{jk} = -\eta \frac{\partial E}{\partial w_{jk}} \quad (9)$$

$\eta \in (0,1)$ is learning rate.

Have the Eq.(6) into the Eq.(9):

$$\Delta w_{jk} = -\eta \frac{\partial E}{\partial w_{jk}} = -\eta \cdot \frac{\partial E}{\partial y_k} \cdot \frac{\partial y_k}{\partial w_{jk}} \quad (10)$$

$$\Delta w_{jk} = \eta \cdot (t_k - y_k) \cdot y_k \cdot (1 - y_k) \cdot y_j \quad (11)$$

among them:

$$\delta_k = (t_k - y_k) \cdot y_k \cdot (1 - y_k) \quad (12)$$

② weigh regulation between the input layer and hidden layer:

$$w_{ij}(t+1) = w_{ij}(t) + \Delta w_{ij} \quad (13)$$

$$\Delta w_{ij} = -\eta \frac{\partial E}{\partial w_{ij}} = \eta \cdot \delta_j \cdot x_i \quad (14)$$

in the Eq.(14):

$$\delta_j = \sum_k \delta_k W_{jk} y_j (1 - y_j) y_i \quad (15)$$

3. BP NETWORK TOOL BOX IN MATLAB

software MATLAB7.0 supply a neural network toolbox(Neural Network Toolbox, for short, NNbox)。Next, aiming at BP network establishment and training, I will introduce how to program with these function, based on NNbox-relating function.

3.1 BP Network Establishment

MATLAB neural network toolbox supplies professional function newff ( )[3] for neural network establishment. The grammar of it is as follows:

net=newff (Xr,[S1 S2 … SN1],{TF1 TF2 … TFN1}, BTF, BLF,PF) (16)

in the Eq.(16) above, Xr is a input vector, which has 2 lines that denotes the minimum and the maximum of the input vector respectively. [S1 S2 … SN1] express, in turn, the unit numbers of the hidden layers and output layers in BP network; {TF1 TF2 … TFN1} represent respectively the functions in the hidden layer and the output layer. The function, such as tansig、logsig and purelin and so on, can be used and 'tansig' is default; BTF, which expresses back train function in network, is character string variable and 'trainlm' is default; BLF, which represents back weigh learnling function, is a character string variable and 'learngdm' is default; PF, which expresses performance function concluding mae (calculating network average absolute error), mser (calculating mean-square error), msereg (calculating mean-square error and the weighting of weigh or threshold value) and sse (calculating network mean-square sum), is a character string variable calculating network output error to provide criterion for training, which chooses 'mse' as default; net is new creating BP neural network. BTF、BLF and PF will be set in terms of requirement ,or omitted.

After defining network structure, newff will automatically transfer the function 'init' with default parameter to initialize each weigh and threshold value in network, which will create a trainable for feedforward network with 'net' as the return value.

Due to the compress effect nonlinear transfer function gives the output, the output layer usually adopts linear transfer function to keep the output range.

3.2 BP Neural Network Train

After new BP network establishment, it's followed to train the BP network, which is with the input and output used in the network, it's in the train process to modify the weigh and threshold continually to make the performance function minimum, which realizes nonlinear image between input and output.

Many learning function and train function in the network are provided in NNbox. Algorithm can be classified into two kinds which are regular gradient descent and modified algorithm.

There are two kinds of patterns about network train pattern in MATLAB: pattern of gradual varying and pattern of batch processing. In the former, when one learning example is input, weigh and threshold value must be modified in terms of the network performance function. In the latter, after all learning examples are input, weigh and threshold value can be just modified according to the network performance function. Nay, with batch processing, it's unnecessary to set train function for connection weigh and threshold values of every layer. Instead, it's the only request to set a train function for the whole network. Seen the two points said above, it's easier to use batch processing. Now, many modified steep train algorithm only adopt batch processing. Whereas, I just discuss batch processing here.

The function used to train network with batch processing is 'train', the transfer format is:

[net, tr]= train(NET, p, t) (17)

in the Eq.(17), p and t express input matrix and output matrix respectively; NET is the net established by function newff; net is the network after training; tr is train record(represent train steps epoch and performance perf).

It's needed to point out: train is used to train in terms of the train function defined in newff. Different train method is corresponded to different training function[4].

Next, take the basic gradient descent method as example to show the train function transfer format:

[w1,b1,w2,b2,te,tr]=trainbp(w1,b1,f1,w2,b2,f2,p,t,tp) (18)

In the Eq.(18), p and t express input and output vector. Te is actual train number, tr is row vector of network train error square-sum, tp represents network train parameters(learning rate、expectation error、maximum learning number and so on).

It's needed to pay more attention to transfer the function name said above directly in training. Before transferring, initialize the variables below:

net.trainParam.show: after how many times, show;

net.trainParam.Lr: learning rate; normally choice range: [0.01~0.7]

net.trainParam.epochs: maximum train times;

net.trainParam.goal: goal function error.

4. APPLICATION EXAMPLES WITH BP NN

BP network is mainly applied to the fields such as function approximation、curve imitation、pattern identification、classification and data compress、image process、system control and so on. There, take two examples to show the convenience BP tool function in MATLAB provides for BP research.

4.1 Curve Imitation

In actual application, it's expected to create some nonlinear input-output curve without exact function connecting. With neural network to realize curve imitation, it's very easy.

```
p=-1:0.1:0.9;
t=[-0.832 -0.423 -0.024 0.344 1.282 3.456 4.02 3.232 2.102
    1.504 0.248 1.242 2.844 2.862 2.052 1.684 1.022 2.224
    3.022 1.984];
```

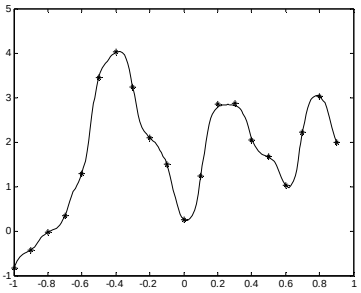


Fig.2. Curve Imitation Simulation

```
net=newff([-1 1],[15 1],{'tansig' 'purelin'},'traingdx',
'learngdm');
net.trainParam.epochs=2500;
net.trainParam.goal=0.001;
net.trainParam.show=10;
net.trainParam.lr=0.05;
net1=train(net,p,t);
plot(p,t,'*');
p=-1:0.01:0.9;
r=sim(net1,p);
hold on
plot(p,r)
hold off
```

4.2 Pattern Identification

The example is to simulate the prediction about some system problem with MATLAB neural network tool box. Three examples are respectively （1 1 0），（0 1 1），（1 0 1），problem codes are（1 0），(0 1)，(1 1)in turn. Next, design、train and simulate with adaptive learning rate backpropagation.

Program is as followed:

```
p=[ 1 1 0; 0 1 1; 1 0 1]';                %P is input
vector
t=[ 1 0; 0 1; 1 1]';                      %T is output
vector
net=newff(minmax(p),[6  2],{'logsig'  'purelin'},'traingdx');
                                  %create a new BP
                                  network
net.trainParam.goal=0.001;          %set network train
goal
net.trainParam.epochs=5000;         %set the maximum
network train time length
net1=train(net,p,t)                 %train network
x=[0.9946 0.99372 0.0013; 0.0005 0.9934 0.9786; 0.9562
0.0043 0.9825]';                    %input validate
example
c=sim(net1,x)                       %network
simulation
```

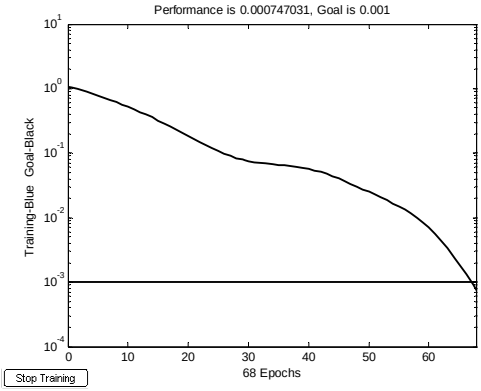


Fig .3. Network Train Error Curve

5. CONCLUSIONS

P neural network is the core of feedforward in artificial neural network. BP tool function in MATLAB supplies great convenience for BP network research. It avoids the complexity of advanced language and easy for users to design and simulate. Seen from the two examples above, satisfactory effect will be gotten with BP tool function.

REFERENCES

[1] Jinkun Liu, *Intelligent Control*, Beijing: Electronic Industrial Public,2005.

[2] Meixian Wu,Xueliang Zhang,"Summarization of BP Neural Networks Improvement,*"Taiyuan University of Science & Technology Transaction*, Vol.26,No.2,2005.

[3] Guoyong Li, *Intelligent Control* Beijing: electronic industrial public,2005.

[4] Xiancai Gui, *realization of BP Networks And Their Application on MATLAB,*Zhanjiang Normal College Transaction Vol.25,No.3,2004.

Jie Chen, Sep. 1958, male, Han nationality, associate professor, research interest in modeling and process contrll.