David Taniar Osvaldo Gervasi
Beniamino Murgante Eric Pardede
Bernady O. Apduhan (Eds.)

LNCS 6019

Computational Science and Its Applications – ICCSA 2010

International Conference
Fukuoka, Japan, March 2010
Proceedings, Part IV

Springer

Lecture Notes in Computer Science 6019

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

David Taniar Osvaldo Gervasi
Beniamino Murgante Eric Pardede
Bernady O. Apduhan (Eds.)

Computational Science and Its Applications – ICCSA 2010

International Conference
Fukuoka, Japan, March 23-26, 2010
Proceedings, Part IV

Springer

Volume Editors

David Taniar
Monash University, Clayton, VIC 3800, Australia
E-mail: david.taniar@infotech.monash.edu.au

Osvaldo Gervasi
University of Perugia, 06123 Perugia, Italy
E-mail: osvaldo@unipg.it

Beniamino Murgante
University of Basilicata, L.I.S.U.T. - D.A.P.I.T., 85100 Potenza, Italy
E-mail: beniamino.murgante@unibas.it

Eric Pardede
La Trobe University, Bundoora, VIC 3083, Australia
E-mail: e.pardede@latrobe.edu.au

Bernady O. Apduhan
Kyushu Sangyo University, Fukuoka 813-8503, Japan
E-mail: bob@is.kyusan-u.ac.jp

Library of Congress Control Number: 2010922807

CR Subject Classification (1998): C.2, H.4, F.2, H.3, C.2.4, F.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-642-12188-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12188-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

These multiple volumes (LNCS volumes 6016, 6017, 6018 and 6019) consist of the peer-reviewed papers from the 2010 International Conference on Computational Science and Its Applications (ICCSA2010) held in Fukuoka, Japan during March 23–26, 2010. ICCSA 2010 was a successful event in the International Conferences on Computational Science and Its Applications (ICCSA) conference series, previously held in Suwon, South Korea (2009), Perugia, Italy (2008), Kuala Lumpur, Malaysia (2007), Glasgow, UK (2006), Singapore (2005), Assisi, Italy (2004), Montreal, Canada (2003), and (as ICCS) Amsterdam, The Netherlands (2002) and San Francisco, USA (2001).

Computational science is a main pillar of most of the present research, industrial and commercial activities and plays a unique role in exploiting ICT innovative technologies. The ICCSA conference series has been providing a venue to researchers and industry practitioners to discuss new ideas, to share complex problems and their solutions, and to shape new trends in computational science.

ICCSA 2010 was celebrated at the host university, Kyushu Sangyo University, Fukuoka, Japan, as part of the university's 50th anniversary. We would like to thank Kyushu Sangyo University for hosting ICCSA this year, and for including this international event in their celebrations. Also for the first time this year, ICCSA organized poster sessions that present on-going projects on various aspects of computational sciences.

Apart from the general track, ICCSA 2010 also included 30 special sessions and workshops in various areas of computational sciences, ranging from computational science technologies, to specific areas of computational sciences, such as computer graphics and virtual reality. We would like to show our appreciation to the workshops and special sessions Chairs and Co-chairs.

The success of the ICCSA conference series, in general, and ICCSA 2010, in particular, was due to the support of many people: authors, presenters, participants, keynote speakers, session Chairs, Organizing Committee members, student volunteers, Program Committee members, Steering Committee members, and people in other various roles. We would like to thank them all. We would also like to thank Springer for their continuous support in publishing ICCSA conference proceedings.

March 2010

Osvaldo Gervasi
David Taniar

Organization

ICCSA 2010 was organized by the University of Perugia (Italy), Monash University (Australia), La Trobe University (Australia), University of Basilicata (Italy), and Kyushu Sangyo University (Japan)

Honorary General Chairs

Takashi Sago	Kyushu Sangyo University, Japan
Norio Shiratori	Tohoku University, Japan
Kenneth C.J. Tan	Qontix, UK

General Chairs

Bernady O. Apduhan	Kyushu Sangyo University, Japan
Osvaldo Gervasi	University of Perugia, Italy

Advisory Committee

Marina L. Gavrilova	University of Calgary, Canada
Andrès Iglesias	University of Cantabria, Spain
Tai-Hoon Kim	Hannam University, Korea
Antonio Laganà	University of Perugia, Italy
Katsuya Matsunaga	Kyushu Sangyo University, Japan
Beniamino Murgante	University of Basilicata, Italy
Kazuo Ushijima	Kyushu Sangyo University, Japan (ret.)

Program Committee Chairs

Osvaldo Gervasi	University of Perugia, Italy
David Taniar	Monash University, Australia
Eric Pardede (Vice-Chair)	LaTrobe University, Australia

Workshop and Session Organizing Chairs

Beniamino Murgante	University of Basilicata, Italy
Eric Pardede	LaTrobe University, Australia

Publicity Chairs

Jemal Abawajy	Deakin University, Australia
Koji Okamura	Kyushu Sangyo University, Japan
Yao Feng-Hui	Tennessee State University, USA
Andrew Flahive	DSTO, Australia

International Liaison Chairs

Hiroaki Kikuchi	Tokay University, Japan
Agustinus Borgy Waluyo	Institute for InfoComm Research, Singapore
Takashi Naka	Kyushu Sangyo University, Japan

Tutorial Chair

Andrès Iglesias	University of Cantabria, Spain

Awards Chairs

Akiyo Miyazaki	Kyushu Sangyo University, Japan
Wenny Rahayu	LaTrobe University, Australia

Workshop Organizers

Application of ICT in Healthcare (AICTH 2010)

Salim Zabir	France Telecom /Orange Labs Japan
Jemal Abawajy	Deakin University, Australia

Approaches or Methods of Security Engineering (AMSE 2010)

Tai-hoon Kim	Hannam University, Korea

Advances in Web-Based Learning (AWBL 2010)

Mustafa Murat Inceoglu	Ege University (Turkey)

Brain Informatics and Its Applications (BIA 2010)

Heui Seok Lim	Korea University, Korea
Kichun Nam	Korea University, Korea

Computer Algebra Systems and Applications (CASA 2010)

Andrès Iglesias	University of Cantabria, Spain
Akemi Galvez	University of Cantabria, Spain

Computational Geometry and Applications (CGA 2010)

Marina L. Gavrilova	University of Calgary, Canada

Computer Graphics and Virtual Reality (CGVR 2010)

Osvaldo Gervasi	University of Perugia, Italy
Andrès Iglesias	University of Cantabria, Spain

Chemistry and Materials Sciences and Technologies (CMST 2010)

Antonio Laganà	University of Perugia, Italy

Future Information System Technologies and Applications (FISTA 2010)

Bernady O. Apduhan	Kyushu Sangyo University, Japan
Jianhua Ma	Hosei University, Japan
Qun Jin	Waseda University, Japan

Geographical Analysis, Urban Modeling, Spatial Statistics (GEOG-AN-MOD 2010)

Stefania Bertazzon	University of Calgary, Canada
Giuseppe Borruso	University of Trieste, Italy
Beniamino Murgante	University of Basilicata, Italy

Graph Mining and Its Applications (GMIA 2010)

Honghua Dai	Deakin University, Australia
James Liu	Hong Kong Polytechnic University, Hong Kong
Min Yao	Zhejiang University, China
Zhihai Wang	Beijing JiaoTong University, China

High-Performance Computing and Information Visualization (HPCIV 2010)

Frank Dévai	London South Bank University, UK
David Protheroe	London South Bank University, UK

International Workshop on Biomathematics, Bioinformatics and Biostatistics (IBBB 2010)

Unal Ufuktepe	Izmir University of Economics, Turkey
Andres Iglesias	University of Cantabria, Spain

International Workshop on Collective Evolutionary Systems (IWCES 2010)

Alfredo Milani	University of Perugia, Italy
Clement Leung	Hong Kong Baptist University, Hong Kong

International Workshop on Human and Information Space Symbiosis (WHISS 2010)

Takuo Suganuma	Tohoku University, Japan
Gen Kitagata	Tohoku University, Japan

Mobile Communications (MC 2010)

Hyunseung Choo	Sungkyunkwan University, Korea

Mobile Sensor and Its Applications (MSIA 2010)

Moonseong Kim	Michigan State University, USA

Numerical Methods and Modeling/Simulations in Computational Science and Engineering (NMMS 2010)

Elise de Doncker	Western Michigan University, USA
Karlis Kaugars	Western Michigan University, USA

Logical, Scientific and Computational Aspects of Pulse Phenomena in Transitions (PULSES 2010)

Carlo Cattani	University of Salerno, Italy
Cristian Toma	Corner Soft Technologies, Romania
Ming Li	East China Normal University, China

Resource Management and Scheduling for Future-Generation Computing Systems (RMS 2010)

Jemal H. Abawajy	Deakin University, Australia

Information Retrieval, Security and Innovative Applications (RSIA 2010)

Mohammad Mesbah Usddin	Kyushy University, Japan

Rough and Soft Sets Theories and Applications (RSSA 2010)

Mustafa Mat Deris	Universiti Tun Hussein Onn, Malaysia
Jemal H. Abawajy	Deakin University, Australia

Software Engineering Processes and Applications (SEPA 2010)

Sanjay Misra	Atilim University, Turkey

Tools and Techniques in Software Development Processes (TTSDP 2010)

Sanjay Misra	Atilim University, Turkey

Ubiquitous Web Systems and Intelligence (UWSI 2010)

David Taniar	Monash University, Australia
Eric Pardede	La Trobe University, Australia
Wenny Rahayu	La Trobe University, Australia

Wireless and Ad-Hoc Networking (WADNet 2010)

Jongchan Lee	Kunsan National University, Korea
Sangjoon Park	Kunsan National University, Korea

WEB 2.0 and Social Networks (Web2.0 2010)

Vidyasagar Potdar	Curtin University of Technology, Australia

Workshop on Internet Communication Security (WICS 2010)

José Maria Sierra Camara	University of Madrid, Spain

Wireless Multimedia Sensor Networks (WMSN 2010)

Vidyasagar Potdar	Curtin University of Technology, Australia
Yan Yang	Seikei University, Japan

Program Committee

Kenneth Adamson	Ulster University, UK
Margarita Albertí Wirsing	Universitat de Barcelona, Spain
Richard Barrett	Oak Ridge National Laboratory, USA
Stefania Bertazzon	University of Calgary, Canada
Michela Bertolotto	University College Dublin, Ireland
Sandro Bimonte	CEMAGREF, TSCF, France
Rod Blais	University of Calgary, Canada
Ivan Blecic	University of Sassari, Italy
Giuseppe Borruso	Università degli Studi di Trieste, Italy
Martin Buecker	Aachen University, Germany
Alfredo Buttari	CNRS-IRIT, France
Carlo Cattani	University of Salerno, Italy
Alexander Chemeris	National Technical University of Ukraine "KPI", Ukraine
Chen-Mou Cheng	National Taiwan University, Taiwan
Min Young Chung	Sungkyunkwan University, Korea
Rosa Coluzzi	National Research Council, Italy
Stefano Cozzini	National Research Council, Italy
José A. Cardoso e Cunha	Univ. Nova de Lisboa, Portugal
Gianluca Cuomo	University of Basilicata, Italy
Alfredo Cuzzocrea	University of Calabria, Italy
Ovidiu Daescu	University of Texas at Dallas, USA
Maria Danese	University of Basilicata, Italy
Pravesh Debba	CSIR, South Africa
Oscar Delgado-Mohatar	University Carlos III of Madrid, Spain
Roberto De Lotto	University of Pavia, Italy

Jean-Cristophe Desplat	Irish Centre for High-End Computing, Ireland
Frank Dévai	London South Bank University, UK
Rodolphe Devillers	Memorial University of Newfoundland, Canada
Pasquale Di Donato	Sapienza University of Rome, Italy
Carla Dal Sasso Freitas	UFRGS, Brazil
Francesco Gabellone	National Research Council, Italy
Akemi Galvez	University of Cantabria, Spain
Marina Gavrilova	University of Calgary, Canada
Nicoletta Gazzea	ICRAM, Italy
Jerome Gensel	LSR-IMAG, France
Andrzej M. Goscinski	Deakin University, Australia
Alex Hagen-Zanker	Cambridge University, UK
Muki Haklay	University College London, UK
Hisamoto Hiyoshi	Gunma University, Japan
Choong Seon Hong	Kyung Hee University, Korea
Fermin Huarte	University of Barcelona, Spain
Andrès Iglesias	University of Cantabria, Spain
Antonio Laganà	University of Perugia, Italy
Mustafa Murat	Inceoglu Ege University, Turkey
Ken-ichi Ishida	Kyushu Sangyo University, Japan
Antonio Izquierdo	Universidad Carlos III de Madrid, Spain
Daesik Jang	Kunsan University, Korea
Peter Jimack	University of Leeds, UK
Korhan Karabulut	Yasar University, Turkey
Farid Karimipour	Vienna University of Technology, Austria
Baris Kazar	Oracle Corp., USA
Dong Seong Kim	Duke University, USA
Pan Koo Kim	Chosun University, Korea
Ivana Kolingerova	University of West Bohemia, Czech Republic
Dieter Kranzlmueller	Ludwig Maximilians University and Leibniz Supercomputing Centre Munich, Germany
Domenico Labbate	University of Basilicata, Italy
Rosa Lasaponara	National Research Council, Italy
Maurizio Lazzari	National Research Council, Italy
Xuan Hung Le	University of South Florida, USA
Sangyoun Lee	Yonsei University, Korea
Bogdan Lesyng	Warsaw University, Poland
Clement Leung	Hong Kong Baptist University, Hong Kong
Chendong Li	University of Connecticut, USA
Laurence Liew	Platform Computing, Singapore
Xin Liu	University of Calgary, Canada
Cherry Liu Fang	U.S. DOE Ames Laboratory, USA
Savino Longo	University of Bari, Italy
Tinghuai Ma	NanJing University of Information Science and Technology, China
Antonino Marvuglia	University College Cork, Ireland

Michael Mascagni	Florida State University, USA
Nikolai Medvedev	Institute of Chemical Kinetics and Combustion SB RAS, Russia
Nirvana Meratnia	University of Twente, The Netherlands
Alfredo Milani	University of Perugia, Italy
Sanjay Misra	Atilim University, Turkey
Asish Mukhopadhyay	University of Windsor, Canada
Beniamino Murgante	University of Basilicata, Italy
Takashi Naka	Kyushu Sangyo University, Japan
Jiri Nedoma	Academy of Sciences of the Czech Republic, Czech Republic
Laszlo Neumann	University of GironAlexey Rodionova, Spain
Belen Palop	Universidad de Valladolid, Spain
Dimos N. Pantazis	Technological Educational Institution of Athens, Greece
Luca Paolino	Università di Salerno, Italy
Marcin Paprzycki	Polish Academy of Sciences, Poland
Gyung-Leen Park	Cheju National University, Korea
Kwangjin Park	Wonkwang University, Korea
Paola Perchinunno	University of Bari, Italy
Carlo Petrongolo	University of Siena, Italy
Antonino Polimeno	University of Padova, Italy
Jacynthe Pouliot	Université Laval, France
David C. Prosperi	Florida Atlantic University, USA
Dave Protheroe	London South Bank University, UK
Richard Ramaroso	Harvard University, USA
Jerzy Respondek	Silesian University of Technology, Poland
Alexey Rodionov	Institute of Computational Mathematics and Mathematical Geophysics, Russia
Jon Rokne	University of Calgary, Canada
Octavio Roncero	CSIC, Spain
Maytham Safar	Kuwait University, Kuwait
Haiduke Sarafian	The Pennsylvania State University, USA
Bianca Schön	University College Dublin, Ireland
Qi Shi	Liverpool John Moores University, UK
Dale Shires	U.S. Army Research Laboratory, USA
Olga Sourina	Nanyang Technological University, Singapore
Henning Sten	Copenhagen Institute of Technology, Denmark
Kokichi Sugihara	Meiji University, Japan
Francesco Tarantelli	University of Perugia, Italy
Jesús Téllez	Universidad Carlos III de Madrid, Spain
Parimala Thulasiraman	University of Manitoba, Canada
Giuseppe A. Trunfio	University of Sassari, Italy
Mario Valle	Swiss National Supercomputing Centre, Switzerland

Pablo Vanegas	Katholieke Universiteit Leuven, Belgium
Piero Giorgio Verdini	INFN Pisa and CERN, Italy
Andrea Vittadini	University of Padova, Italy
Koichi Wada	University of Tsukuba, Japan
Krzysztof Walkowiak	Wroclaw University of Technology, Poland
Jerzy Wasniewski	Technical University of Denmark, Denmark
Robert Weibel	University of Zurich, Switzerland
Roland Wismüller	Universität Siegen, Germany
Markus Wolff	University of Potsdam, Germany
Kwai Wong	University of Tennessee, USA
Mudasser Wyne	National University, USA
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Albert Y. Zomaya	University of Sydney, Australia

Sponsoring Organizations

ICCSA 2010 would not have been possible without the tremendous support of many organizations and institutions, for which all organizers and participants of ICCSA 2010 express their sincere gratitude:

University of Perugia, Italy
Kyushu Sangyo University, Japan
Monash University, Australia
La Trobe University, Australia
University of Basilicata, Italia
Information Processing Society of Japan (IPSJ) - Kyushu Chapter
and with IPSJ SIG-DPS

Table of Contents – Part IV

Workshop on Chemistry and Materials Sciences and Technologies (CMST 2010)

Workshop on Biomathematics, Bioinformatics and Biostatistics (IBBB 2010)

Workshop on Human and Information Space Symbiosis (IWHISS 2010)

Workshop on Information Retrieval, Security and Innovative Applications (RSIA 2010)

Workshop on Collective Evolutionary Systems (IWCES 2010)

General Track on Computational Methods, Algorithms and Applications

Accurate Quantum Dynamics on Grid Platforms: Some Effects of Long Range Interactions on the Reactivity of N + N_2

Sergio Rampino[1], Ernesto Garcia[2], Fernando Pirani[1], and Antonio Laganà[1]

[1] Università degli Studi di Perugia, Dipartimento di Chimica, Via Elce di Sotto 8, 06123 Perugia, Italia
[2] Universidad del Pais Vasco, Departamento de Quimica Fisica, Paseo de la Universidad 7, 01006 Vitoria, España

Abstract. The potential energy surface of the N + N_2 atom diatom system has been reformulated using the LAGROBO functional form for interpolating ab initio points in the short distance region and using a modified Lennard Jones functional form to model the van der Waals interaction at long range. On the proposed surface extended quantum calculations have been performed using the European Grid platform. The values of the calculated thermal rate coefficients fairly reproduce the experimental results.

Keywords: Reactive scattering, quantum dynamics and kinetics, nitrogen exchange reaction, state specific reaction probabilities, thermal rate coefficients.

1 Introduction

The exchange and dissociation reactions of the nitrogen atom - nitrogen molecule system play a primary role in the modeling of spacecraft reentry [1]. Both the heat load and the reactivity of the species produced by the shock wave are, in fact, important data for heat shield design since nitrogen is the major component of Earth's atmosphere. Reactions of nitrogen are also important in other high temperature environments involving N_2, as, for example, shock tube experiments [2]. Experimental measurements of the N + N_2 thermal rate coefficients are available at the temperatures of 3400 and 1273 K [3,4,5].

The significant progress made in the last decades in computing the properties of atom diatom exchange reactions using quantum means has made it possible to calculate related detailed reactive probabilities and (by properly averaging them) thermal rate coefficients. A crucial step of the theoretical study is the assemblage of an accurate potential energy surface (PES). For this reason in the recent past extended ab initio calculations led to the formulation of the WSHDSP [6] and the L4 [7] PESs. On both PESs extended quantum calculations have been performed to the end of evaluating the thermal rate coefficient at the temperature of the experiments. Unfortunately, calculated values differ orders of magnitude from available experimental data not confirming the claimed accuracy of the proposed PESs.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 1–12, 2010.

For this reason in the work reported here we exploit the flexibility of the LAGROBO (Largest Angle Generalization of the ROtating Bond Order) functional form [7,8,9] to lower the minimum energy profile of the L4 PES and we incorporate an accurate description of the atom diatom long range interaction. On the resulting PES (ML4LJ), a computational campaign has been carried out to calculate the thermal rate coefficients using the time independent quantum reactive scattering program ABC [10] implemented on the section of the production computing Grid of EGEE [11] accessible to the COMPCHEM [12] virtual organization.

Accordingly, the article is organized as follows. In Sect. 2, the reasons for reformulating the N_3 interaction are illustrated. In Sect. 3, the computational machinery is described. In Sect. 4, calculated values of the rate coefficient are compared to experimental data.

2 Modeling the Interaction

A LEPS PES was the first functional formulation of the interaction for the N + N_2 system to ever appear in the literature [13]. Such PES has a saddle to reaction associated with a symmetric collinear ($\widehat{\mathrm{NNN}} = 180°$) geometry. The ab initio finding of a bent ($\widehat{\mathrm{NNN}} \simeq 120°$) geometry at the saddle to reaction was reported first in Refs. [14,15]. This proved the inadequacy of the LEPS PES to describe correctly the main features of the strong interaction region of the reaction channel and motivated the development of a new functional representation of the PES called L3 and based on the LAGROBO formulation [16].

More recently new high-level ab initio calculations have been performed for three thousand geometries of the N + N_2 system [6], and calculated values have been fitted using the unpublished WSHDSP functional form. The WSHDSP PES exhibits the peculiar feature of leading to a minimum energy path showing two fairly high barriers sandwiching a shallow well. The same high level ab initio approach was followed by us to generate the L4 PES [7] based also on the LAGROBO functional form and having similar characteristics. The failure of quantum results to reproduce the measured values of the thermal rate coefficient prompted an extended analysis of the detailed state to state probabilities. The analysis showed that, despite the different reactivities of N + N_2 on the L4 and on the WSHDSP PES, on both surfaces the calculations underestimate the measured value of the rate coefficient mainly because of the same strong interaction region shape [17].

In this paper we describe the assemblage of the ML4LJ PES for which, following the suggestions of [14,15], we adopt a lower energy value for the minimum energy path in the strong interaction region and add a properly parametrized Lennard Jones tail in the long range region.

2.1 The LAGROBO Formulation

The procedure followed to lower the potential energy in the strong interaction region exploits the flexibility of the LAGROBO functional form (V^{LAGROBO})

adopted to formulate the already mentioned L4 PES. The LAGROBO functional form is, in fact, built out of a combination of the ROtating Bond Order (ROBO) [8] V_τ^{ROBO} model potentials associated with the description of the various (τ) exchange processes allowed for the considered system as follows:

$$V^{\mathrm{LAGROBO}}(r_{\tau,\tau+1}, r_{\tau+1,\tau+2}, r_{\tau+2,\tau}) = \sum_\tau w(\Phi_\tau) V_\tau^{\mathrm{ROBO}}(\rho_\tau, \alpha_\tau, \Phi_\tau) \ . \tag{1}$$

In (1) $r_{\tau,\tau+1}$ is the internuclear distance of the $\tau, \tau+1$ diatom with $\tau = 1$ for the A + BC arrangement while ρ_τ and α_τ are the hyperradius and hyperangle of the hyperspherical BO (HYBO) coordinates defined as

$$\rho_\tau = (n_{\tau+2,\tau}^2 + n_{\tau,\tau+1}^2)^{1/2} \text{ and } \alpha_\tau = \arctan[n_{\tau,\tau+1}/n_{\tau+2,\tau}] \ . \tag{2}$$

In (2) $n_{\tau,\tau+1} = \exp[-\beta_{\tau,\tau+1}(r_{\tau,\tau+1} - r_{\mathrm{eq}\tau,\tau+1})]$ is the BO coordinate of the $\tau, \tau+1$ diatom with the process index τ being cyclic of module 3 and indicating the exchanged atom. The weight function $w(\Phi_\tau)$ of (1) is such as to privilege the ROBO potential better representing the overall interaction as the related Φ_τ (the angle formed by the two (broken and formed) bonds having in common the atom τ) varies [16]. It is defined as

$$w(\Phi_\tau) = \frac{u(\Phi_\tau)}{\sum_\tau u(\Phi_\tau)} \ , \tag{3}$$

with $u(\Phi_\tau)$ being a damping function of the type

$$u(\Phi_\tau) = \frac{1}{2}\left(1 + \tanh\left[\gamma_\tau(\Phi_\tau - \Phi_\tau^\circ)\right]\right) \tag{4}$$

(because of the symmetry of the system we assign the same values 50 and 75° for γ and Φ° and whenever possible we drop the subscript τ). The functional representation given to the ROBO potential in HYBO coordinates is:

$$V^{\mathrm{ROBO}}(\rho, \alpha, \Phi) = a_1(\alpha, \Phi)\left[2\frac{\rho}{a_2(\alpha, \Phi)} - \frac{\rho^2}{a_2^2(\alpha, \Phi)}\right] \tag{5}$$

where $a_1(\alpha, \Phi)$ describes the dependence of the well depth of the fixed Φ minimum energy path (MEP) of the exchange process, while the function $a_2(\alpha, \Phi)$ describes the location on ρ of the minimum of the fixed Φ MEP of the exchange process.

To make the LAGROBO functional form reproduce both the regions of the ab initio potential energy values bearing a single and a double barrier MEP, as in Ref. [7] the a_1 function was given the formulation

$$\begin{aligned} a_1(\alpha, \Phi) = & -D_{\mathrm{N}_2} + b_{10}(\Phi) + b_{12}(\Phi)(\alpha - 45^\circ)^2 \\ & + \left(\frac{-b_{10}(\Phi) - b_{12}(\Phi)\ (45^\circ)^2}{(45^\circ)^4}\right)(\alpha - 45^\circ)^4 \ , \end{aligned} \tag{6}$$

where

$$b_{10}(\Phi) = c_{100} + c_{102}(\Phi - 118.6^\circ)^2 + c_{103}(\Phi - 118.6^\circ)^3 \tag{7}$$

and

$$b_{12}(\Phi) = c_{120} + c_{121}\Phi + c_{122}\Phi^2 \ , \tag{8}$$

while the a_2 function was given the formulation

$$\begin{aligned} a_2(\alpha,\Phi) = {} & b_{20}(\Phi) + b_{22}(\Phi)(\alpha - 45^\circ)^2 \\ & + \left(\frac{3 - 3\ b_{20}(\Phi) - 2\ b_{22}(\Phi)\ (45^\circ)^2}{(45^\circ)^4} \right) (\alpha - 45^\circ)^4 \\ & + \left(\frac{-2 + 2\ b_{20}(\Phi) + b_{22}(\Phi)\ (45^\circ)^2}{(45^\circ)^6} \right) (\alpha - 45^\circ)^6 \ , \end{aligned} \tag{9}$$

where

$$b_{20}(\Phi) = c_{200} + c_{201}\Phi + c_{202}\Phi^2 + c_{203}\Phi^3 \tag{10}$$

and

$$b_{22}(\Phi) = c_{220} + c_{221}\Phi + c_{222}\Phi^2 \ . \tag{11}$$

As apparent from the formulation given above the symmetry of the system is reflected by the expansion in $\alpha - 45^\circ$ while the transition state angle is 118.6° and has an energy of 1.45 eV. Thanks to this formulation of the LAGROBO potential all the parameters of the ML4LJ PES take the same values of those of Ref. [7] except c_{100} (that quantifies the height of the C_{2v} well above the N + N_2 asymptote) that was given the value of 1.45 eV.

The key features of the strong interaction region of the ML4LJ PES are illustrated in the third column of Table 1, where the geometry and the potential energy V of the system at the reaction saddles (labeled by s) and at the bottom of the intermediate well (labeled by w) of the MEP are reported. For comparison the corresponding values of the WSHDSP and the L4 PESs are also shown.

2.2 The Empirical Long Range Attractive Tail

A first attempt to add a long range tail to the L4 PES was reported in Ref. [17]. It consisted in switching at long range from the LAGROBO to a more appropriate functional form, as done for the WSHDSP PES where the long range tail of Ref. [18] was added. More in detail, the long range attractive tail was expressed

Table 1. Key features of the reaction channels of the potential energy surfaces of N + N_2 ("s" stands for saddle, "w" for well). The geometry of the second saddle (the well is sandwiched by two symmetric barriers) is obtained by switching the values of r_{12} and r_{23} for the saddle reported.

	WSHDSP		L4		ML4LJ	
	s	w	s	w	s	w
r_{12}/bohr	2.23	2.40	2.24	2.40	2.23	2.40
r_{23}/bohr	2.80	2.40	2.77	2.40	2.82	2.40
Φ/degrees	119	120	116.7	118.6	116.4	118.6
V/eV	2.05	1.89	2.06	1.93	1.60	1.45

in terms of a linear combination of R^{-n} terms ($n = 6, 8, 10, 12$) with R being the atom diatom distance. The dependence of the related coefficients on the angle γ formed by R with the diatom internuclear distance r was expressed in terms of Legendre polynomials, while no dependence on r was assumed (as in Ref. [18]). To smoothly connect the short range behaviour to the long range one, the R^{-n} terms were scaled at $R = 4$ bohr to reproduce the L4 value, with the switch from L4 to R^{-n} being performed in an interval of about 1 bohr.

For the ML4LJ PES, instead, the functional representation of the Improved Lennard-Jones (ILJ) [19] model was adopted at long range. The ILJ potential model has the general form

$$V(R,\gamma) = \varepsilon(\gamma)\left[\frac{6}{n(R,\gamma)-6}\left(\frac{R_{\rm m}(\gamma)}{R}\right)^{n(R,\gamma)} - \frac{n(R,\gamma)}{n(R,\gamma)-6}\left(\frac{R_{\rm m}(\gamma)}{R}\right)^{6}\right] , \tag{12}$$

where $\varepsilon(\gamma)$ and $R_{\rm m}(\gamma)$ represent, respectively, the depth of the van der Waals potential well and its location in R. In (12), the first term describes the R-dependence of the repulsion, while the second one represents the R-dependence of the long-range attraction. The $n(R,\gamma)$ term depends on R as

$$n(R,\gamma) = \beta + 4.0\left(\frac{R}{R_{\rm m}(\gamma)}\right)^2 , \tag{13}$$

where β is a factor related to the hardness of the two interacting partners and is expected to vary in a limited range when passing from one system to another, bearing a specific trend. If n is assumed to be independent of R, (12) becomes identical to the usual LJ(n,6) model.

For all values of the orientation angle γ, the potential parameters are defined as

$$\begin{aligned} R_{\rm m}(\gamma) &= R_{\rm m\parallel}\cos^2\gamma + R_{\rm m\perp}\sin^2\gamma \ , \\ \varepsilon(\gamma) &= \varepsilon_{\parallel}\cos^2\gamma + \varepsilon_{\perp}\sin^2\gamma \ . \end{aligned} \tag{14}$$

The values β, $R_{\rm m\parallel}$, $R_{\rm m\perp}$, $\varepsilon_{\parallel}$ and $\varepsilon_{\perp}$ (given in Table 2) have been obtained following the guidelines reported in Refs. [19,20,21,22,23].

In Fig. 1 the energy profile of the ILJ model potential calculated for different values of γ is plotted as a function of R. As shown in the figure the profile lowers in energy at short range in moving from collinear ($\gamma = 0°$) to perpendicular ($\gamma = 90°$) approaches. On the contrary, the long range tail becomes less attractive in the same interval of γ values.

3 The Computational Machinery

The computational machinery adopted for the present study follows that of GEMS [24]. In other words, the computational procedure carries out first the ab initio calculation of the electronic energy at a properly chosen grid of molecular geometries, then fits the calculated potential energy values to a suitable functional form and integrates on it the equations of motion in their quantum version

Table 2. Empirical parameters for the ILJ long range attractive tail

β	8.2
$\varepsilon_{\parallel}$/meV	5.81
$R_{\mathrm{m}\parallel}$/bohr	7.710
$\varepsilon_{\perp}$/meV	9.77
$R_{\mathrm{m}\perp}$/bohr	6.763

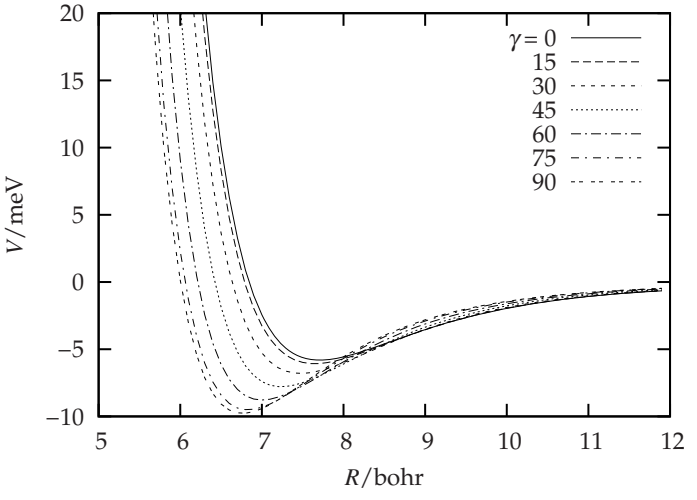


Fig. 1. Energy profile of the ILJ potential plotted as a function of the atom-diatom coordinate R for various values of the orientation angle γ, at the equilibrium diatomic internuclear distance r

to determine the relevant scattering **S** matrix (the probability **P** matrix elements are the square moduli of those of **S**). The last step consists in averaging over the unobserved variables to assemble out of the state to state **S** matrix elements the ab initio estimates of the relevant experimental observables like the thermal rate coefficient reported in this paper.

3.1 The Calculation of Detailed Quantum Probabilities

For the evaluation of quantum detailed reaction probabilities use was made of the program ABC [10], based on a time independent hyperspherical coordinate method. ABC integrates the atom-diatom Schrödinger equation for all the reactant states of a given total energy E and a fixed value of the total angular momentum (**J**) quantum number J (see Ref. [25] for more details). To this end, ABC expands the fixed E nuclei wavefunction ψ in terms of the hyperspherical arrangement channel (τ) basis functions $B^{JM}_{\tau v_\tau j_\tau K_\tau}$ labeled after J, M and K_τ (the space- and body-fixed projections of the total angular momentum **J**), v_τ and j_τ (the τ asymptotic vibrational and rotational quantum numbers), and depending on both the three Euler angles and the internal Delves hyperspherical angles. In order to carry out the fixed E and J propagation of the solution from

small to asymptotic values of hyperradius ρ (not to be confused with the ρ of the HYBO coordinates defined in (2) since ρ is now defined as $\rho = (R_\tau^2 + r_\tau^2)^{1/2}$) one needs to integrate the equations

$$\frac{\mathrm{d}^2\mathbf{g}(\rho)}{\mathrm{d}\rho^2} = \mathbf{O}^{-1}\mathbf{U}\mathbf{g}(\rho) \ . \tag{15}$$

In (15) $\mathbf{g}(\rho)$ is the matrix of the coefficients of the expansion of ψ, $\mathbf{O}$ is the overlap matrix and $\mathbf{U}$ is the coupling matrix defined as

$$U^{\tau' v'_\tau j'_\tau K'_\tau}_{\tau v_\tau j_\tau K_\tau} = \langle B^{JM}_{\tau v_\tau j_\tau K_\tau} | \frac{2\mu}{\hbar^2}(\bar{H} - E) - \frac{1}{4\rho^2} | B^{JM}_{\tau' v'_\tau j'_\tau K'_\tau} \rangle \ , \tag{16}$$

with μ being the reduced mass of the system and $\bar{H}$ the set of terms of the Hamiltonian operator not containing derivatives with respect to ρ. In ABC the integration of (15) is performed by segmenting the ρ interval into several ρ sectors inside each and through which the solution matrix is propagated from the ρ origin to its asymptotic value where the $\mathbf{S}$ matrix is determined [26]. This fixed E and J calculation is recursive and represents, therefore, the basic computational grain of the ABC program to iterate when computing the state specific probabilities and the thermal rate coefficient.

Actually, because of the large number of involved partial waves associated with the heavy mass of N + N_2 when dealing with the calculation of the rate coefficient, the approximation of evaluating the reactive probabilities associated with $J \neq 0$ by adopting the popular J-shifting model [27,28] was introduced. More in detail, in the J-shifting model the non zero J probabilities are approximated by properly shifting in energy the $J = 0$ ones ($P^{J=0}(E)$) as follows:

$$P^{JK}(E) = P^{J=0}(E - \Delta E^{JK}) \ , \tag{17}$$

with ΔE^{JK} being defined as

$$\Delta E^{JK} = \bar{B}J(J+1) + (A - \bar{B})K^2 \ . \tag{18}$$

This formula is based on the approximation that the geometry of the system at the bent saddle is a symmetric top one. In (18) $\bar{B} = (B + C)/2$ with A, B and C being the three rotational constants of the triatom at the saddle. In the J-shifting approximation the thermal rate coefficient is in fact written as

$$k(T) = \frac{1}{hQ_\mathrm{R}} \sum_{J=0}^{\infty}(2J+1) \sum_{K=-J}^{J} \int_0^\infty e^{-E/k_\mathrm{B}T} \sum_{v,j} \sum_{v',j'} P^{J=0}_{vj \to v'j'}(E - \Delta E^{JK}) \, \mathrm{d}E \ , \tag{19}$$

where h is Planck's constant and Q_R is the total atom-diatom partition function of the reactants at temperature T per volume unit defined as

$$Q_\mathrm{R} = \left(\frac{2\pi\mu_{\mathrm{N,N_2}} k_\mathrm{B} T}{h^2}\right)^{3/2} \left(\sum_{v,j}(2j+1)e^{-\epsilon_{vj}/k_\mathrm{B}T}\right) \ , \tag{20}$$

with k_B being the Boltzmann constant.

3.2 The Computing Grid Distribution Model

As already mentioned, the present study was made possible by an intensive exploitation of the Grid to calculate single E, single J **S** matrix elements for the N + N_2 reaction. A general scheme for the concurrent reorganization of the related computer programs on the Grid is the following: a distribution procedure iterates over the E, J pairs to perform the recursive integration of (15). Accordingly, the computation is articulated as a coarse grained uncoupled loop and its distributed execution model is typical of the "parameter sweeping" type. To this end, a procedure able to handle large sets of jobs was developed. Each job execution requires the sending to the Grid of an execution script, of a specific input file and of the ABC scattering program. The execution script is the same for all jobs while the input file is different for each job. In order to better cope with the heterogeneous nature of both the computing hardware and software (compilers, libraries, submission systems, etc.) of the Grid, executable rather than source programs were distributed over the net. In fact, in spite of the fact that the time required for sending the source code is considerably shorter than that required for sending its executable (this procedure is also more selective in terms of the type of machine to adopt) this approach exploits the fact that there is no need for identifying the compiler of each machine, selecting the optimal options for compilation, compiling the code and verifying that all runs give exactly the same results as the ones obtained on the original machine.

In this work, only $J = 0$ calculations were performed: 160 single energy calculations were run concurrently in clusters of 10, thus gaining a speedup of about 16 (the overhead related to the Grid handling of the jobs is negligible with respect to the execution time of each cluster (on the average 34 hours)).

4 Results and Conclusions

As already mentioned, an extended campaign of calculations was performed at null total angular momentum for a fine grid of total energy values (energy was varied from 1.6 eV to 3.2 eV in steps of 0.01 eV). The hyperradius was varied up to 12.0 bohr and divided into 150 sectors. Basis functions with internal energy below 4.0 eV and maximum rotational quantum number 90 were all considered for the expansion.

4.1 Detailed Probabilities

For illustrative purpose we plot in Fig. 2 the state specific reactive probabilities calculated at $v = 0$ and $j = 0$ on the L4 and the ML4LJ PES. As already mentioned the ML4LJ PES was obtained by lowering the energy profile of the L4 PES (thus obtaining a ML4 PES) and adding an ILJ attractive tail. We also plot the probabilities calculated for the ML4 PES, where the long range attractive tail is not taken into account. As apparent from the figure, while the variation of the MEP in going from L4 to ML4LJ varies substantially the threshold though

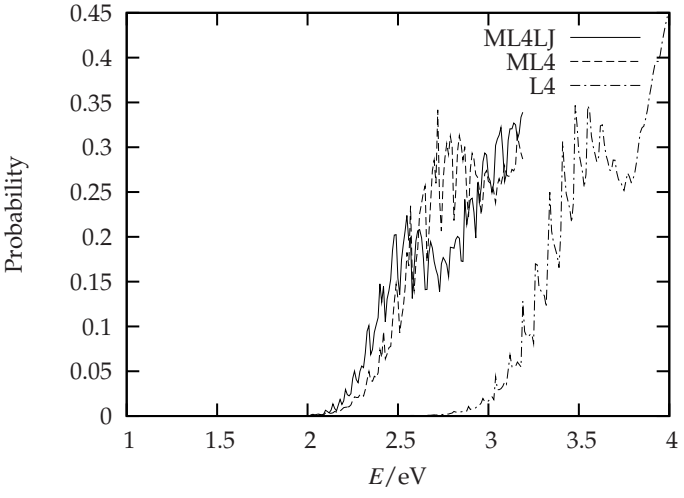


Fig. 2. Ground state specific reaction probabilities calculated on the ML4LJ (solid line), ML4 (dashed line) and L4 (dashed-dotted line) potential energy surfaces plotted as a function of total energy

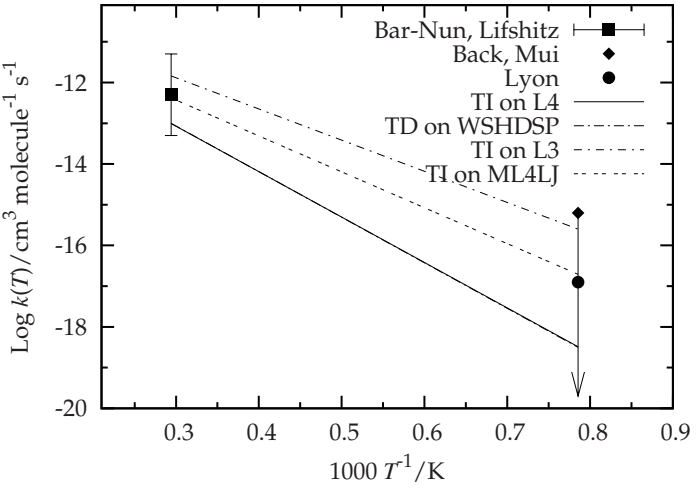


Fig. 3. Logarithm of the J-shifting rate coefficient calculated for the exchange N + N_2 reaction on the ML4LJ (dashed line), L3 (dashed-dotted line), L4 and WSHDSP (solid and dashed-dotted superimposed lines) PESs plotted as a function of the inverse temperature. The ML4LJ, L3 and L4 values were calculated with the time independent (TI) ABC program, while the WSHDSP values were obtained with a time dependent (TD) technique and reported in Ref.[6]. Experimental data of Refs. [3,4,5] are also shown. Note that the two experiments performed at $T = 1273$ K only give upper limits for the rate coefficient.

preserving the detailed structure of the state specific probabilities, adding a long range attractive tail does not vary the threshold yet enhances the low energy reactivity (as previously found for the L4 and L4w PESs of Ref. [17]). If the MEP shape is left unchanged, the resonant structure is preserved.

4.2 Thermal Rate Coefficients

The values of the thermal rate coefficients of the N + N_2 reaction calculated at the temperatures of the experiment (1273 K and 3400 K [3,4,5]) on the L3 [29], L4, WSHDSP and the present PES (ML4LJ) are shown in Fig. 3 (the values calculated on the ML4 are not shown here because they do not appreciably differ from those calculated on the ML4LJ PES). Note that the L4 and WSHDSP (solid and dahsed-dotted, respectively, superimposed lines) results underestimate the experimental values. The ML4LJ results give instead a larger value of the rate coefficient well in line with the lowering of the MEP and a better agreement with the experimental data. However, one has to be cautious in using this alignment to accredit ML4LJ as the best available PES since similar improvements could be obtained in other ways and the comparison with the experiment relies on the J-shifting approximation whose validity has still to be assessed.

Acknowledgments

Partial financial support from EGEE III, COST (D37 Gridchem), ESA ESTEC Contract 21790/08/NL/HE, ARPA Umbria, MICINN (CTQ2008-02578/BQU) and MIUR is acknowledged.

References

1. Armenise, I., Capitelli, M., Celiberto, R., Colonna, G., Gorse, C., Laganà, A.: The effect of N+N_2 collisions on the non-equilibrium vibrational distributions of nitrogen under reentry conditions. Chemical Physics Letters 227, 157–163 (1994)
2. Armenise, I., Capitelli, M., Garcia, E., Gorse, C., Laganà, A., Longo, S.: Deactivation dynamics of vibrationally excited nitrogen molecules by nitrogen atoms. effects on non-equilibrium vibrational distribution and dissociation rates of nitrogen under electrical discharges. Chemical Physics Letters 200, 597–604 (1992)
3. Back, R.A., Mui, J.Y.P.: The reactions of active nitrogen with $N^{15}O$ and N_2^{15}. Journal of Physical Chemistry
4. Bar-Nun, A., Lifshitz, A.: Kinetics of the homogeneous exchange reaction: $^{14-14}N_2$ + $^{15-15}N_2$ → 2 $^{14-15}N_2$. single-pulse shock-tube studies. Journal of Chemical Physics 47, 2878–2888 (1967)
5. Lyon, R.: Search for the N-N_2 exchange reaction. Canadian Journal of Chemistry 50, 1433–1437 (1972)
6. Wang, D., Stallcop, J.R., Huo, W.M., Dateo, C.E., Schwenke, D.W., Partridge, H.: Quantal study of the exchange reaction for N + N_2 using an ab initio potential energy surface. Journal of Chemical Physics 118, 2186–2189 (2003)
7. Garcia, E., Saracibar, A., Gómez Carrasco, S., Laganà, A.: Modeling the global potential energy surface of the N + N_2 reaction from ab initio data. Physical Chemistry Chemical Physics 10, 2552–2558 (2008)

8. Laganà, A.: A rotating bond order formulation of the atom diatom potential energy surface. Journal of Chemical Physics 95, 2216–2217 (1991)
9. Laganà, A., Ferraro, G., Garcia, E., Gervasi, O., Ottavi, A.: Potential energy representations in the bond order space. Chemical Physics 168, 341–348 (1992)
10. Skouteris, D., Castillo, J.F., Manolopoulos, D.E.: ABC: a quantum reactive scattering program. Computer Physics Communications 133, 128–135 (2000)
11. EGEE: Enabling grids for e-science in europe, http://www.eu-egee.org
12. Laganà, A., Riganelli, A., Gervasi, O.: On the Structuring of the Computational Chemistry Virtual Organization COMPCHEM. In: Gavrilova, M.L., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganà, A., Mun, Y., Choo, H. (eds.) ICCSA 2006. LNCS, vol. 3980, pp. 665–674. Springer, Heidelberg (2006)
13. Laganà, A., Garcia, E., Ciccarelli, L.: Deactivation of vibrationally excited nitrogen molecules by collision with nitrogen atoms. Journal of Physical Chemistry 91, 312–314 (1987)
14. Petrongolo, C.: MRD-CI ground state geometry and vertical spectrum of N_3. Journal of Molecular Structure 175, 215–220 (1988)
15. Petrongolo, C.: MRD-CI quartet potential surfaces for the collinear reactions N (^4S_u) + N_2 ($X^1\Sigma_g^+$, $A^3\Sigma_u^+$, and $B^3\Pi_g$). Journal of Molecular Structure (Teochem) 202, 135–142 (1989)
16. Garcia, E., Laganà, A.: The largest angle generalization of the rotating bond order potential: the H + H_2 and N + N_2 reactions. Journal of Chemical Physics 103, 5410–5416 (1995)
17. Rampino, S., Skouteris, D., Laganà, A., Garcia, E., Saracibar, A.: A comparison of the quantum state-specific efficiency of N + N_2 reaction computed on different potential energy surfaces. Physical Chemistry Chemical Physics 11, 1752–1757 (2009)
18. Stallcop, J.R., Partridge, H., Levin, E.: Effective potential energies and transport cross sections for atom-molecule interactions of nitrogen and oxygen. Physical Review A 64, 042722–1–12 (2001)
19. Pirani, F., Brizi, S., Roncaratti, L.F., Casavecchia, P., Cappelletti, D., Vecchiocattivi, F.: Beyond the Lennard-Jones model: a simple and accurate potential function probed by highly resolution scattering data useful for molecular dynamics simulations. Physical Chemistry Chemical Physics 10, 5489–5503 (2008)
20. Cambi, R., Cappelletti, D., Liuti, G., Pirani, F.: Generalized correlations in terms of polarizability for van der waals interaction potential parameter calculations. Journal of Chemical Physics 95, 1852–1861 (1991)
21. Pirani, F., Cappelletti, D., Liuti, G.: Range, strength and anisotropy of intermolecular forces in atom-molecule systems: an atom-bond pairwise additivity approach. Chemical Physics Letters 350, 286–296 (2001)
22. Capitelli, M., Cappelletti, D., Colonna, G., Gorse, C., Laricchiuta, A., Liuti, G., Longo, S., Pirani, F.: On the possibility of using model potentials for collision integral calculations of interest for planetary atmospheres. Chemical Physics 338, 62–68 (2007)
23. Cappelletti, D., Pirani, F., Bussery-Honvault, B., Gomez, L., Bartolomei, M.: A bond-bond description of the intermolecular interaction energy: the case of weakly bound N_2-H_2 and N_2-N_2 complexes. Physical Chemistry Chemical Physics 10, 4281–4293 (2008)
24. Laganà, A.: Towards a grid based universal molecular simulator. In: Theory of the dynamics of elementary chemical reactions, pp. 363–380. Kluwer, Dordrecht (2004)
25. Schatz, G.C.: Quantum reactive scattering using hyperspherical coordinates: results for H + H_2 and Cl + HCl. Chemical Physics Letters 150, 92–98 (1988)

26. Pack, R.T., Parker, G.A.: Quantum reactive scattering in three dimensions using hyper-spherical (APH) coordinates. theory. Journal of Chemical Physics 87, 3888–3921 (1987)
27. Bowman, J.M.: Reduced dimensionality theory of quantum reactive scattering. Journal of Physical Chemistry 95, 4960–4968 (1991)
28. Bowman, J.M.: Approximate time independent methods for polyatomic reactions. Lecture Notes in Chemistry 75, 101–114 (2000)
29. Laganà, A., Faginas Lago, N., Rampino, S., Huarte-Larrañaga, F., Garcia, E.: Thermal rate coefficients in collinear versus bent transition state reactions: the N + N_2 case study. Physica Scripta 78, 058116–1–9 (2008)

Supporting Molecular Modeling Workflows within a Grid Services Cloud

Martin Koehler[1], Matthias Ruckenbauer[2,3], Ivan Janciak[1], Siegfried Benkner[1], Hans Lischka[3], and Wilfried N. Gansterer[2]

[1] University of Vienna, Faculty of Computer Science
Department of Scientific Computing, Austria
[2] University of Vienna, Faculty of Computer Science
Research Lab CTA, Austria
[3] University of Vienna, Institute for Theoretical Chemistry, Austria
koehler@par.univie.ac.at, matthias.ruckenbauer@par.univie.ac.at,
janciak@par.univie.ac.at, sigi@par.univie.ac.at,
hans.lischka@univie.ac.at, wilfried.gansterer@univie.ac.at

Abstract. Seamless integrated support for scientific workflows accessing HPC applications, deployed on globally distributed computing resources, has become a major challenge in scientific computing. Scientific workflows in the domain of theoretical chemistry are typically long running, deal with huge files, and have a need for dynamic execution control mechanisms. In this paper, we describe a service-oriented approach based on the Vienna Grid Environment (VGE) that tackles these challenges by seamlessly integrating the Ubuntu Cloud infrastructure supporting the scheduling of dynamic and partitioned workflows. The VGE service environment, which enables the provisioning of HPC applications and data sources as Web services, has been enhanced with support for virtualized workflows. The generic scientific workflow infrastructure is utilized in the context of the CPAMMS project, an interdisciplinary research initiative in the area of computational molecular modeling and simulation. A case study implementing a complex scientific workflow for computing photodynamics of biologically relevant molecules, a simulation of the nonadiabatic dynamics of 2,4-pentadieneiminum-cation (Protonated Schiff Base 3, PSB3) solvated in water, is realized via the presented infrastructure.

1 Introduction

Resources for high performance computing (HPC) applications in the modern scientific world are often not concentrated and available at one location but rather distributed, often globally, over a multitude of sites, each with its individual architecture, features and limitations. Grid computing research investigated the provisioning of safe, but still easy and transparent access to such resources for a long time. Traditional grid computing tools as [1], [2] provide access to distributed high performance computing infrastructures. Jobs are submitted, often through a web service interface, and scheduled transparently to resources in the Grid on the fly. On the other hand, the Software as a Service (SaaS) approach

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 13–28, 2010.

enables transparent access to remote applications, or more specifically in the Grid context, to computationally demanding scientific codes, via Web service interfaces. Some of the authors of this paper have earlier addressed the problem of providing access to scientific resources, in the context of molecular modeling, successfully using Web-service based technologies with VGE [4].

Computational campaigns in molecular science often involve several programs with varying interdependence on the different outputs. Especially in the field of molecular modeling and molecular dynamics, many time-consuming and data-intensive computations have to be performed. Most investigations do not only involve a single execution of scientific applications (mostly highly complex parallel codes), but rather a workflow with inputs for one calculation being used as or depending on the output of others. Installation, configuration and optimization of these codes on specific HPC resources is a demanding task, and the resulting binaries are often very tightly bundled to the architecture they were built for. Because of this the traditional Grid computing approach to submit the code with the job and compile it on the fly is not favorable in the context considered here.

The emergence of Cloud computing extends and complements the traditional Grid approach with support of Software/Platform/Infrastrucutre as a Service (SaaS, PaaS, and IaaS), also often referred to as *aaS. Cloud computing provides a shared infrastructure to its customers by utilizing virtualization technologies and allows them to host their own software/platform/infrastructure on a rental basis. As cloud computing enables transparent and dynamic hosting of applications together with their native execution environment without knowledge about the actual hardware infrastructure, an efficient execution of scientific codes on such an infrastructure poses many new challenges.

Due to the dynamic characteristics of workflows in the domain of computational molecular modeling and because of the unpredictable runtime and resource requirements of these workflows, the provisioning of scientific workflows as workflow services in the cloud, where resources can be made available on demand, seems a promising approach. Our work integrates a workflow enactment engine into the VGE and prepares the middleware for hosting workflow services transparently in the cloud. Following the cloud and Web service paradigms, a cloud image for hosting scientific workflows virtualized as services has been developed. The cloud image includes all the required software packages allowing an easy deployment of new scientific workflows as Web services by leveraging cloud technologies.

Scientific workflows usually include many potentially long running scientific codes, each of them exposed as a service, which may be invoked many times during a specific workflow. To make use of the dynamic resource allocation possibilities in the cloud, our workflow services are able to delegate these requests to basic service invocation cloud images. This leads to a decentralized execution of the workflow in the cloud environment and allows to schedule the different service invocations to different cloud image instances. An on the fly mechanism that optimizes the utilization of cloud resources during the workflow execution can be implemented on top of this mechanism.

An important goal of our work is to implement an infrastructure for executing complex and long running scientific workflows based on the needs of domain scientists. Our infrastructure is presented by using a case study workflow implemented together with scientists of the molecular modeling domain. The scientific algorithm used in the case study statistically evaluates results of a multitude of independent computations. This algorithm is only meaningful in a statistical sense and for an unknown system it is usually not clear from the beginning how many computations will be necessary to obtain a good statistic for the result. Confronted with limited computational resources one tries to limit this number to an absolute minimum. Utilizing dynamic workflow mechanisms allows the evaluation of intermediate results during the workflow execution and the automatic termination, if a needed statistical certainty is reached. The number of invocations of scientific codes is unpredictable but dependent on the intermediate results.

2 Basic Technologies

2.1 Vienna Grid Environment

The Vienna Grid Environment (VGE) [3],[5] has been developed in the context of Grid computing for facilitating transparent access to parallel applications on remote high performance and high throughput computing systems. Compute intensive applications, often highly optimized parallel MPI or OpenMP codes, available on clusters or other HPC systems can be made available over the Internet to clients as application services within a service-oriented Grid architecture. Application services include support for dynamic negotiation of service-level-agreements based on a flexible QoS infrastructure using business models specialized for the application. A generic Web service interface for managing the job execution on remote resources hides the details of the applications execution environment. The uniform interface offers common operations for uploading input data, starting remote job execution, querying the state of the execution, downloading the results, and support for push and pull input or output files (up to several GB) directly between application services or Web storage resources.

In addition to application services VGE provides data services to facilitate access to and integration of heterogeneous data sources. Data services are built upon OGSA-DAI and OGSA-DQP and offer transparent access to multiple data sources via a virtual global schema relying on flexible data mediation techniques.

In this work VGE was enhanced with support of scientific workflows based upon the WEEP Workow Engine [6]. Workflow services enable the virtualization of complex scientific workflows that comprise multiple application services each realized as a VGE service and deployed in a Cloud.

2.2 Workflow Enactment Engine

In this section we present a workflow enactment engine named WEEP Engine, which is used to orchestrate Web services involved in the CPAMMS workflow. It is a WS-BPEL[1] compliant workflow engine being developed at the Institute of Scientific Computing as a part of the Globus incubation project[2]. The main goal of the project is to implement a modern enactment engine for service-oriented environments leveraging the latest Grid and Web technologies. Hence, the implementation of the engine follows the latest WSRF standard, which defines stateful Web services that store the state of their operations and other properties without breaking the compatibility to standard WS-I services.

The WEEP Engine supports fault tolerant and dynamic orchestration of Web services by dynamic evaluation of their WSDL documents. In addition, during the runtime the engine can modify endpoint references of the involved services and this way it supports requirements of dynamic scientific workflows. Since the WEEP Engine uses its own invocation mechanism, this exchange of service endpoints can be done by direct modification of SOAP messages. In order to stay compatible with WS-BPEL specification, the WEEP Engine uses standard language constructs (i.e. assign/copy) to update the requested information in a header of the SOAP messages. For complex scientific workflows such as the one from computational chemistry considered in this paper, typically nested loops are required. The WEEP Engine supports also this feature and also by evaluating service responses it can dynamically modify the number of iterations. Parallel execution of loops is supported as well.

One of the advantages of WS-BPEL is that it can be used to represent any process as a composite Web service with its own WSDL interface. This feature allows for hiding a complex process behind a simple service operation, and therefore the WEEP Engine also enables a hierarchical composition of the deployed workflows. This feature is also used in the workflow considered in this paper by implementing the concepts of external and internal workflows. These capabilities are used to provide a flexible load balancing mechanism of workflow executions at execution time.

2.3 Cloud Environment

Cloud Computing allows developers to provide their services over the Internet in a scalable way based on virtualized resources without a need of investing into new hardware infrastructure. As defined in [7] Cloud computing subsumes Software as a Service (SaaS) and Utility computing and refers therefore to both the applications delivered as services and the hardware and system software used for hosting the services. According to [7], a *public cloud* as a cloud made available to the public using a pay-as-you-go manner. A *private cloud* is referred to as a cloud used in a company or university but not made available to the public.

[1] WS-BPEL Version 2.0: http://www.oasis-open.org/specs/index.php#wsbpelv2.0
[2] http://dev.globus.org

In our work we utilized the Ubuntu Enterprise Cloud infrastructure[3], which allows an easy deployment of a private cloud environment and which is based on Eucalyptus[8], an open source system for providing private and hybrid cloud systems. Eucalyptus provides Amazon EC2, S3, and EBS[4] compatible interfaces, which allow the deployment of Amazon EC2 images and the usage of Amazon client toolkits to manage and maintain instances. The cloud environment is structured in a front-end server and clusters comprised of nodes. The front-end system runs an Eucalyptus-cloud service. Every cluster runs an instance of the Eucalyptus cluster controller and can be configured with several nodes using the Eucalyptus node controller service.

3 Architecture

An architectural overview of our infrastructure for scientific workflows is depicted in Figure 1. As shown, a private cloud environment based on the Ubuntu Enterprise Cloud and the integrated Eucalyptus software is used as basic infrastructure. The private cloud environment hosted at the University of Vienna includes one *Cloud Frontend* server with an Eucalyptus Cloud Controller installation capable of the management of available resources and of the deployment of new image instances. A PC cluster of Eucalyptus Nodes (for simplicity only *Eucalyptus Node 1*, *Eucalyptus Node 2* are shown) and a *Cluster Frontend* server is used for the execution and hosting of image instances. Two preconfigured virtual machine images (workflow service cloud image, basic service invocation image), based on a minimal Ubuntu Server 9.04 installation and created with KVM virtualization technology, are provided. Both images can be hosted on a PC with virtualization capabilities, and can be easily deployed in an Ubuntu Enterprise Cloud installation or to Amazon EC2. In Figure 1 an instance of the workflow service cloud image is hosted on *Eucalyptus Node 1* including a workflow service virtualizing the computational molecular modeling workflow described in this paper. *Eucalyptus Node 2* hosts an instance of the basic service invocation image supporting access to a single VGE application service.

3.1 Basic Service Invocation Cloud Image

A basic service invocation workflow encapsulates the life cycle of accessing a VGE service and is deployed as web service in the *basic service invocation image*. A simple interface is provided by the service invocation workflow which can be used by workflow designers during the workflow development process. The basic workflow constitutes an additional abstraction layer hiding the details of accessing and querying a specific application service from the workflow designer. Multiple instances of the basic service invocation image are hosted in the cloud environment and can be used to realize a distributed execution of different service invocations.

The basic service invocation image hosts a WEEP Engine installation exposed via Globus Toolkit 4. The WEEP Engine relies on Java 5, Apache Ant 1.7,

[3] Ubuntu Enterprise Cloud: http://www.ubuntu.com/cloud
[4] Amazon EC2: http://aws.amazon.com/ec2

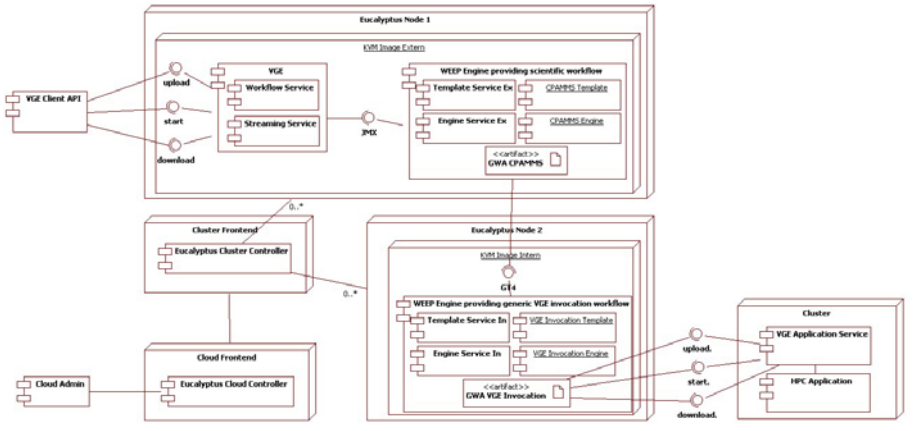


Fig. 1. Scientific Workflow Infrastructure - Deployment Diagram

and on Maven 2.x. WEEP provides a Template Service for the deployment of a generic workflow description (Grid Workflow Archive - gwa) and an Engine Service capable of the creation of an instance of a deployed workflow. Using GT4, WEEP is able to host a workflow as Web service behind a WSDL interface.

The life cycle of accessing a VGE service is hidden behind the generic workflow interface (`BasicVGEInterface`) and shown in Figure 2. The interface describes only a single operation
(`void invokeService()`) for invoking the workflow. The operation needs input information about the service URL (the VGE service which is to be invoked), input file references, input file names, and output file names, and replies with URLs to all defined output files. The workflow dynamically selects the VGE service, which is invoked by this workflow, from the input message. For this reason the workflow can be used for the invocation of any VGE service. The workflow starts with uploading all input file references provided in the input message to the VGE service using the pull mechanism. After the VGE service has been started, a loop querying the state of the execution is performed. When the VGE service is finished, URLs to all defined output files are created and stored in the output message. This allows orchestrating the file transfers between application services dynamically without a need to process the potentially huge files in the workflow engine.

3.2 Workflow Service Cloud Image

The workflow service cloud image can be used to deploy scientific workflows as VGE services without the need of additional software installation. The Workflow service cloud image, based on a Ubuntu Server installation, is configured with a VGE service provisioning environment as described in Section 2.1. The service provisioning environment includes a preconfigured VGE workflow service definition which allows the deployment of a workflow service simply by the

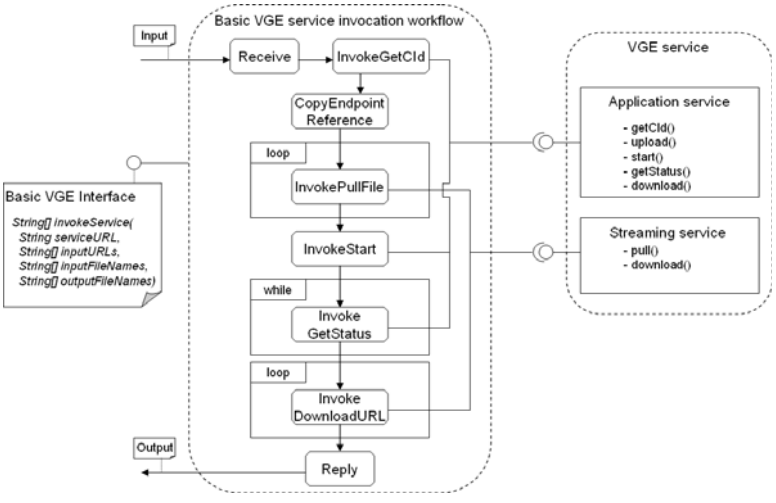


Fig. 2. Basic VGE Service Invocation Workflow

provisioning of a WEEP Grid workflow archive (gwa) including the BPEL process definition. Using the VGE deployment tool, the VGE workflow service can be deployed automatically by providing the reference to the used gwa. The deployed VGE service comprises a workflow service component, virtualizing a workflow behind the generic VGE interface, and a streaming service enabling direct file transfers between services based on a push/pull mechanism. The workflow service automatically deploys the provided gwa in a local WEEP Engine installation accessible via a JMX interface. A WEEP template service is instantiated for the gwa, and a engine service is created, when the workflow is started. It is possible to host several VGE workflow services in one workflow service image. The VGE workflow service is configured with an advanced WebPortal allowing live logging, online user management, and a push/pull mechanism supporting large data transfers directly between services.

Workflow designers use the workflow service cloud image to deploy their scientific workflows based on the generic service invocation image. This allows the definition of scientific workflows on an abstract level based on the simple interface only needing information about the service URL, the input files, and the output files. Additionally the workflow service is able to schedule the possibly long running application service invocations to multiple instances of the basic service invocation image by following a round robin strategy.

4 Computational Molecular Modeling Workflow

One prototypical workflow which occurs in computational molecular dynamics is the pattern of actions that has to be taken when simulating nonadiabatic excited state molecular behavior in a solvent.

The initial position, orientation and velocity of molecules one can obtain is usually not equilibrated and thermalized, i.e. the molecules do not have a distribution that fits to the parameters (temperature, pressure, etc.) of the investigated system. There are various ways to overcome this defect. In gas phase dynamics (without a solvent) the force constant matrix for the whole molecule can be calculated ab-initio and a quantum harmonic oscillator be applied. This is not feasible for solvated dynamics with many molecules because the computational effort to calculate the force constants increases rapidly with the number of atoms (usually $O(N^2)$ to $O(N^6)$). A commonly used method to obtain initial conditions here would be the computation a dynamics run in the ground state while applying a thermostat during which the molecules adapt themselves to their surroundings, and, after this thermalization, pick random (geometry/velocity) points from this trajectory. These points can be used as initial conditions for the excited state dynamics.

For systems bigger than a few lightweight atoms nonadiabatic dynamics cannot be performed any more for the full wavefunction. Tully proposed a scheme for nonadiabatic dynamics which is called the "Tully's fewest switches algorithm" [9]. For this a multitude of independent dynamic runs has to be performed where each trajectory can, due to a 'hopping probability' change from one electronic state to another during the dynamics. The overall result is obtained from the statistics over all trajectories. It cannot be clearly predicted for a system, how many trajectories are needed for a good statistic. The number of trajectories usually calculated here is more or less 'as much as possible', limited by the hardware, i.e., by the number of available processors.

The scenario investigated in this paper is a simulation of the nonadiabatic dynamics of 2,4-pentadieneiminum-cation [10] (Protonated Schiff Base 3, PSB3), solvated in water. We assumed that a limiting number of maximum 10 processors are available simultaneously. This is a realistic quantity for a smaller cluster which is used by many scientific users at the same time. At the same time it is a number much smaller than the expected number of trajectories to be run for a statistically meaningful result.

A thermalized initial solvent geometry from a Monte Carlo simulation was available at the beginning, so the primary thermalization-run was only needed to obtain adapted velocities. The workflow is supposed to perform the complete sequence of actions required for this simulation, including the generation of initial conditions for the first structure by applying random velocities, carrying out the ground-state trajectories with thermostat, picking random points for the initial conditions of the nonadibatic dynamics, and finally computing nonadiabatic dynamic runs on all available processors (see Section 4 and Figure 3). Every time a nonadibatic trajectory ends without error an analysis of all trajectories yet obtained is performed and due to the development of a pre-defined parameter it is decided whether more trajectories are to be computed for a good result or not. The scientific applications to be orchestrated during the specified workflow in the context of molecular science are highly complex and historically grown codes and have been virtualized as VGE application services. The

scientific workflow is mainly based on the NEWTON-X application [11] which is a general-purpose program package for nonadibatic excited-state molecular dynamics. It provides routines for all parts of a molecular dynamics investigation beginning from the generation of initial conditions to the statistical analysis of the results. NEWTON-X uses third-party programs for the calculation of energies, gradients and nonadibatic couplings. For this work the program packages COLUMBUS [12] and TINKER [13] are used in a QM/MM scheme for nonadiabatic dynamics including solvent effects.

4.1 Experimental Setup

In this work the services are deployed on clusters of the University of Vienna, such as the Luna cluster and the local cluster of the QCCD-workgroup at the Department for Theoretical Chemistry. The Luna cluster is hosted at the Department of Scientific Computing and consists of 72 SUN Fire X-4100 servers with two Dual-Core AMD opteron 275 processors and 8 GB of memory. The cluster has totally 288 cores and 576 GB of memory connected via Ethernet and Infiniband. The QCCD-cluster is a heterogenous workstation-cluster with currently 90 processors in 36 nodes ranging from Intel PentiumIV-em64t and AMD Opteron64 to Intel Quad Core i7, all with minimum 2GB, maximum 4GB memory per processor and 3TB filespace for users. Each node has a scratch disc with at least 200 GB. The nodes are connected via Ethernet.

A private cloud environment based on Ubuntu Enterprise Cloud has been installed at the Department of Scientific Computing and is made available securely via the Internet. The Cloud infrastructure is based on one cloud controller computer hosting the cloud environment frontend and the cloud image storage. The cloud controller is able to distribute the cloud image to one cluster of five Intel Quad-Core PCs with each four GB of RAM. The basic setup runs the workflow service cloud image on one cluster node and two generic VGE service image instances on other cloud nodes.

4.2 VGE Application Services For Molecular Science

The grid services used by this scientific workflow were developed over the last years by domain scientists from the field of quantum chemistry and deployed on different cluster systems. The NEWTON-X related services are separated for the different actions NEWTON-X can perform. They are intended to be used on a cluster with batch-queue. Submission scripts have to be provided for each system where the service is deployed.

NX-initcond generates initial conditions due to the input sent. 'Normal' usage of this service requires no special resources and can be executed on the node hosting the service. If, however, the calculation of excitation energies is requested the need for high computional power arises and the job is submitted to a batch-queue.

NX-makedir generates the directory structure and files needed for running Newton-X dynamics. It requires the output of NX-initicond and additional user input (the template setup for the trajectories). The requirements for this procedure are low and it can be performed on the node hosting the service.

NX-runtrajectory accepts multiple dynamic inputs as provided by NX-makedir. Each Newton-X dynamic input found is submitted to the queue as single job. Each of these trajectories runs on a single processor, completely independent of the others. 2GB of main memory and up to 10GB of temporary disc space will be needed for each trajectory. Depending on the system involved each trajectory will need an overall computation time ranging from a few hours up to multiple weeks or months.

NX-diagnostics requires the output of multiple Newton-X dynamic runs and an additional user-defined input. The service performs a diagnostic over the trajectories stating in its output up to which point each of the calculations can be considered reliable for the statistics.

NX-analysis requires the output of multiple Newton-X dynamics, additional user input and optional the output of NX-diagnostics. The service calculates statistics for the provided trajectories as requested in the user-input. It involves statistical analysis based on parsing and rewriting of huge output files (up to a few GBs). Depending on the local setup and architecture it is normally necessary to let this be executed on a seperate computing node.

Additionally, a service has been deployed that derives a subset of parameters from the output of the analysis. From the development of these parameters with increasing number of trajectories the workflow dynamically decides whether more calculations are needed or not. The Tully algorithm for the simulation of nonadiabatic dynamics is only meaningful in a statistical sense and for an unknown system it is usually not clear from the beginning how many trajectories will be necessary to obtain a good statistic for the result. Confronted with limited computational resources one tries to limit this number to an absolute minimum. An additional VGE service is deployed as datacenter hosting the input files and used as storage location for the output files. The file store service stores input and output files on a client session basis. The workflow service orchestrates file transfers between the services. The workflow service handles only file references and files are never transferred through the workflow services which minimizes the needed file transfers.

4.3 Workflow Definition

The structure of the scientific workflow based on the VGE service invocation workflow computing nonadiabatic dynamics of 2,4-pentadieneiminum-cation is shown in Figure 3. The execution of the workflow uses VGE scientific application services for molecular science and includes dynamic workflow control mechanisms

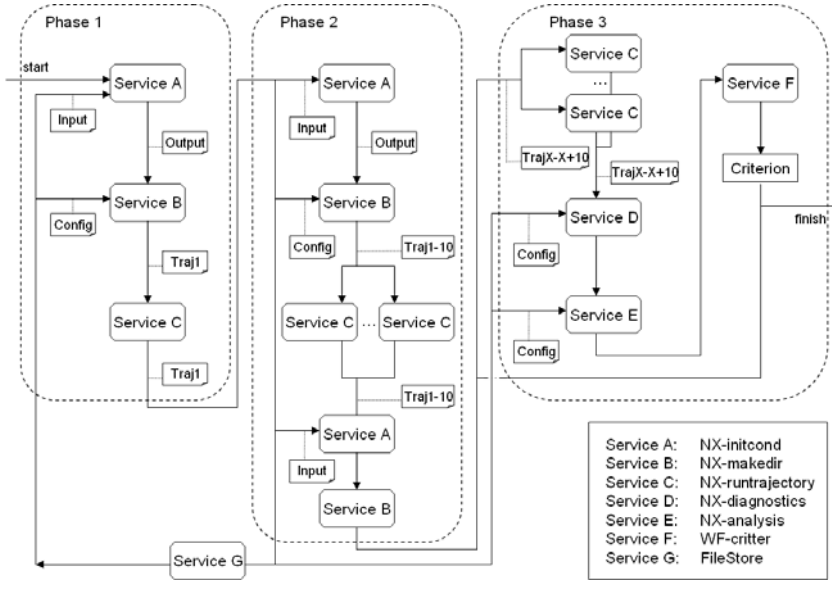


Fig. 3. Scientific Workflow Description

based on intermediate results of the services. The workflow itself is structured in three main phases. The first phase deals with the generation of initial conditions and computes the ground state of the trajectory thus obtaining adapted velocities by invoking the services NX-initcond, NX-makedir and NX-runtrajectory. Input files are transferred from the file storage service to the VGE application services and outputs are directly pulled from the services itself. In the next step ten trajectories are computed based on the initial ground state. From these trajectories the starting points for the computation of the overall problem can be selected. Phase three includes the non-adiabatic simulation of the molecule. This is done by computing additional trajectories based on the initial conditions obtained before until a threshold is reached. The additionally computed trajectories are revised by the NX-diagnostics service and declined, if they include errors. To achieve a good result with minimum computational effort, a parameter (in this case the average excited state lifetime of all till then finished trajectories) is computed with NX-analysis service and monitored by the workflow. This value converges with an increasing number of computed trajectories towards its final value. In a dynamic loop based on this parameter it is decided whether more trajectories have to be computed or not. Therefore the workflow compares the parameters of the last three iterations and terminates the loop if the change in the parameter does not exceed a certain threshold. If the state of the computed trajectories has stabilized, phase three is finished and the results can be downloaded.

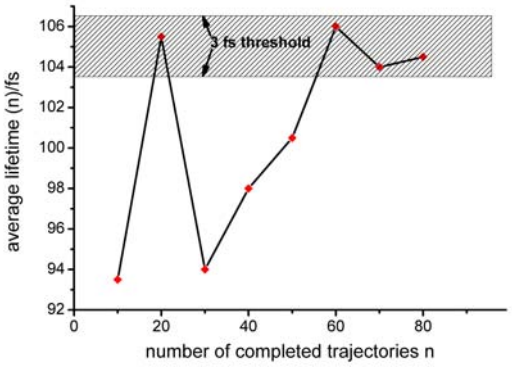


Fig. 4. Development of average lifetime with the number of computed trajectories. Workflow execution was terminated when the lifetime had stabilized within 3fs over 3 consecutive executions.

4.4 Experimental Results

The criterion for termination of the workflow execution was based on the excited state lifetime of the trajectories. When the statistical analysis of all (cumulated) trajectories computed to this point gave for three consecutive executions of the main loop an absolute variation in the lifetime of not more than 3fs, the dynamic study was considered finished (see Figure 4).

As the figure shows 80 nonadiabatic trajectories are needed to retrieve a stable result. Therefore 121 Grid service invocations are necessary, divided as follows: Phase one: 3, Phase two: 14, Phase three: 104. The service invocations are distributed to both basic service invocation images in equal parts. The adiabatic groundstate trajectories of phase one and two need alltogether 81 hours to compute 10 trajectories and pick the initial conditions from. Phase three has to execute 80 trajectories of which each requires in average 8.8 hours computation time. The workflow computes 10 trajectories in parallel during phase three, which leads to an execution time of about 71 hours, including analysis of the results.

5 Related Work

There are many other workflow engines available and some of them are successfully used in business as well as in scientific applications. The engines use different modeling languages and use different planning and scheduling mechanisms or target different environments. A detailed survey of available workflow engines is given in [14,15]. The ActiveBPEL Engine [16] is a Business Process Management runtime environment for executing process definitions created to the WS-BPEL 2.0 and BPEL4WS 1.1 specifications. It is also based on Axis 2.0 and is released

under the GPL license. The advantage of the ActiveBPEL is that it provides an integrated development environment for building, testing and deploying BPEL-based applications. Taverna [17] is an open source grid-aware workflow management system that enables scientists to compose and execute scientific worfklows. The composition is done manually using a graphical user interface. Taverna has become a popular tool in bioinformaticians tool for extracting information data stored in distributed databases often in incompatible formats. The workbench provides a set of transparent, loosely-coupled, semantically-enabled middleware to support scientists that perform data-intensive in-silico experiments on distributed resources, predominantly in the Life Sciences but also in research in psychiatry, chemistry and engineering. The workbench has been developed as part of myGrid project and relies on XML-based SCUFL language.

A project dealing with scientific workflows in the chemical and physical domain is GEMSTONE [18] which provides an integrated framework for accessing Grid resources and workflow enactment based on INFORMNET [19]. GEMSTONE provides rich client interfaces for applications and is based on Firefox. The GEMSTONE client interface follows an application specific approach while VGE provides a generic application independent client API but it is possible to access VGE services using the GEMSTONE client. INFORMNET uses an XML schema workflow language whereas WEEP Engine is based on WS-BPEL specification. Our system additionally supports partitioned workflow executions in a cloud environment. The UNICORE middleware [20] is a framework for scientific and commercial applications and provides an environment for integration of the different tasks as simulations, database access or data acquisition. UNICORE supports workflows in the form of an oriented acyclic graph, each node in the graph represents a single task and allows conditional execution and loops. The Gridbus [21] Workflow Engine (GWFE) facilitates users to link standalone applications and execute their workflow applications on Grids. GWFE provides an XML-based workflow language for the users to define tasks and dependencies. It also supports a just in-time scheduling system, thus allowing the resource allocation decision to be made at the time of task execution and hence adapt to changing grid environments. The latest version GWFE2.0beta has been integrated into Gridbus Broker and supports multiple Grid middleware including GT4.0 Gram Service, PBS, and Sun Grid Engine. In [22] they analyze the differences between running scientific workflows in the Grid and in the cloud from the perspective of domain scientists. The focus is on the execution of jobs in the cloud while our work is dealing with the execution of the workflow itself in the cloud, not the jobs. The work presented in [23] is based on Pegasus and DAGMan (Directed Acyclic Graph Manager) which allows meta-scheduling of a directed acyclic graph of program executions with underlying condor installations. Pegasus itself is a workflow mapping engine supporting automatic mapping of high-level workflow descriptions onto distributed infrastructures. In contrast to our approach DAGMan orchestrates condor job definitions and not invocations of generic Web services. LEAD [24] is a service oriented

infrastructure adaptively utilizing distributed resources, sensors and workflows, driven by a real time event architecture, allowing dynamically adaptive weather analysis and forecasting. A workflow engine based on BPEL is included and notifications are supported for adaptive workflows. On the contrary, our solution adapts the workflow execution based on intermediate results of the scientific applications without notification, but based on a partitioned workflow architecture.

6 Conclusion and Future Work

Investigations of scientists in the domain of molecular science often involve multiple complex programs available on distributed HPC resources with interdependences on inputs and outputs. Enabling easy access via Web services to these programs and to workflows representing the work normally done by hand is a well known approach. Scientific workflows are often restricted by the available computing resources and therefore dynamic mechanisms for automatically supervising and adapting the used resources are needed. Our work describes a use case of the molecular modeling domain with need for automating the execution of long running HPC applications by utilizing dynamic workflow execution mechanisms. Due to the dynamic structure of the workflow it is not possible to completely predict its runtime. Efficient resource usage, and even more service administration, are important issues for service providers. Cloud computing allows service developers to provide Web services in a scalable way based on virtualized resources. We described a workflow service architecture that utilizes a cloud environment and supports the partitioning of workflows. The preparation of preconfigured cloud images for the service provisioning simplifies the service administration and allows the migration or duplication of cloud instances on demand.

The emerging cloud computing technologies enable service providers to easily deploy, migrate, or to duplicate servers without a need of investing into new hardware infrastructure, and allow the appliance of adaptive load balancing strategies based on cloud images. The dynamic characteristics of complex scientific workflows lead to an unpredictable number of VGE service invocations during the workflow execution, which affects the resource usage of basic service invocation cloud instances in an unforeseeable manner. Applying adaptive technologies for the management of a complex IT infrastructure, as a workflow service based on a cloud environment, seems a promising approach for automatically minimizing the resource usage or the costs of a workflow execution in the cloud. Additionally, the migration of scientific applications or data sources in the cloud is possible, as already discussed in [22].

Acknowledgments. This work was partially supported by the research project FS397001 “CPAMMS” within the research focus area Computational Science of the University of Vienna and by the COST Action D37 (Gridchem).

References

1. Foster, I.: Globus toolkit version 4: Software for service-oriented systems. In: Jin, H., Reed, D., Jiang, W. (eds.) NPC 2005. LNCS, vol. 3779, pp. 2–13. Springer, Heidelberg (2005)
2. EGEE Project: gLite - Ligthweight Middleware for Grid Computing, http://glite.web.cern.ch/glite/
3. Benkner, S., Brandic, I., Engelbrecht, G., Schmidt, R.: VGE - A Service-Oriented Grid Environment for On-Demand Supercomputings. In: Proceedings of the Fifth IEEE/ACM International Workshop on Grid Computing (Grid 2004), Pittsburgh, PA, USA, November 2004. IEEE, Los Alamitos (2004)
4. Ruckenbauer, M., Brandic, I., Benkner, S., Gansterer, W., Gervasi, O., Barbatti, M., Lischka, H.: Nonadiabatic Ab Initio Surface-Hopping Dynamics Calculation in a Grid Environment - First Experiences. In: Gervasi, O., Gavrilova, M.L. (eds.) ICCSA 2007, Part I. LNCS, vol. 4705, pp. 281–294. Springer, Heidelberg (2007)
5. Benkner, S., Engelbrecht, G., Köhler, M., Wöhrer, A.: Virtualizing Scientific Applications and Data Sources as Grid Services. In: Cao, J. (ed.) Cyberinfrastructure Technologies and Applications. Nova Science Publishers, New York (2009)
6. Janciak, I., Kloner, C., Brezany, P.: Workflow Enactment Engine for WSRF-Compliant Services Orchestration. In: The 9th IEEE/ACM International Conference on Grid Computing (2008)
7. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. In: Grid Computing Environments Workshop, GCE 2008, pp. 1–10 (2008)
8. Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youse, L., Zagorodnov, D.: The eucalyptus open-source cloud-computing system. In: Cloud Computing and Applications 2008, CCA 2008 (2008)
9. Hammes-Schiffer, S., Tully, J.: Proton-Transfer in Solution - Molecular-Dynamics With Quantum Transitions. Journal of Chemical Physics 101(6), 4657–4667 (1994)
10. Migani, A., Robb, M., Olivucci, M.: Relationship between photoisomerization path and intersection space in a retinal chromophore model. Journal of the American Chemical Society 125(9), 2804–2808 (2003)
11. Barbatti, M., Granucci, G., Persico, M., Ruckenbauer, M., Vazdar, M., Eckert-Maksic, M., Lischka, H.: The on-the-fly surface-hopping program system NEWTON-X: Application to ab initio simulation of the nonadiabatic photodynamics of benchmark systems. Journal of Photochemistry and Photobiology A-Chemistry 190(2-3), 228–240 (2007)
12. Lischka, H., Shepard, R., Brown, F., Shavitt, I.: New Implementation of the Graphical Unitary-Group Approach for Multi-Reference Direct Configuration-Interaction Calculations. International Journal of Quantum Chemistry (suppl. 15), 91–100 (1981)
13. Ponder, J., Richards, F.: An Efficient Newton-Like Method for Molecular Mechanics Energy Minimization of Large Molecules. Journal of Computational Chemistry 8(7), 1016–1024 (1987)
14. Taylor, I., Deelman, E., Gannon, D., Shields, M.: Workflows for e-Science: Scientific Workflows for Grids. Springer-Verlag New York, Inc., Secaucus (2007)
15. Yu, J., Buyya, R.: A taxonomy of scientific workflow systems for grid computing. SIGMOD Rec. 34(3), 44–49 (2005)
16. Active Endpoints: ActiveBPEL Engine (March 2008), http://www.active-endpoints.com

17. Wolstencroft, K., Oinn, T., Goble, C., Ferris, J., Wroe, C., Lord, P., Glover, K., Stevens, R.: Panoply of utilities in taverna. In: E-SCIENCE 2005: Proceedings of the First International Conference on e-Science and Grid Computing, Washington, DC, USA, pp. 156–162. IEEE Computer Society, Los Alamitos (2005)
18. Baldridge, K., Bhatia, K., Greenberg, J., Stearn, B., Mock, S.: Gemstone: Grid-enabled molecular science through online networked environments. In: Invited paper: LSGRID Proceedings (2005)
19. Baldridge, K., Greenberg, J., Sudholt, W., Mock, S., Altintas, I., Amoreria, C., Potier, Y., Birnbaum, A., Bhatia, K.: The computational chemistry prototyping environment. In: Special Issue of the Proceedings of the IEEE on Grid Computing (2005)
20. Erwin, D., Snelling, D.: Unicore: A grid computing environment. In: Sakellariou, R., Keane, J.A., Gurd, J.R., Freeman, L. (eds.) Euro-Par 2001. LNCS, vol. 2150, p. 825. Springer, Heidelberg (2001)
21. Buyya, R., Venugopal, S.: The Gridbus Toolkit for Service Oriented Grid and Utility Computing: An Overview and Status Report. In: 1st IEEE International Workshop on Grid Economics and Business Models, GECON 2004, Seoul, Korea, April 23, pp. 19–36. IEEE CS, Los Alamitos (2004)
22. Hoffa, C., Mehta, G., Freeman, T., Deelman, E., Keahey, K., Berriman, B., Good, J.: On the Use of Cloud Computing for Scientific Workflows. In: IEEE Fourth International Conference on eScience (eScience 2008), Indianapolis, USA, December 7-12 (2008)
23. Deelman, E., Blythe, J., Gil, Y., Kesselman, C., Mehta, G., Patil, S., Su, M., Vahi, K., Livny, M.: Mapping scientific workflows onto the grid. In: Across Grids Conference, Nicosia, Cyprus (2004)
24. Plale, B., Gannon, D., Brotzge, J., Droegemeier, K., Kurose, J., McLaughlin, D., Wilhelmson, R., Graves, S., Ramamurthy, M., Clark, R., Yalda, S., Reed, D., Joseph, E., Chandrasekar, V.: Casa and lead: Adaptive cyberinfrastructure for real-time multiscale weather forecasting. Computer 39(11), 56–64 (2006)

Distributed and Collaborative Learning Objects Repositories on Grid Networks

Simonetta Pallottelli[1], Sergio Tasso[1], Nicola Pannacci[1], Alessandro Costantini[1,2], and Noelia Faginas Lago[2]

[1] Department of Mathematics and Computer Science, University of Perugia
via Vanvitelli, 1, I-06123 Perugia, Italy
{simona,sergio}@unipg.it, nicola.pannacci@gmail.com
[2] Department of Chemistry, University of Perugia
via Elce di Sotto, 8, I-06123 Perugia, Italy
{alex,noelia}@dyn.unipg.it

Abstract. The paper deals with the design and a prototype implementation of a collaborative repository of scientific learning objects based on an efficient mechanism of filing and retrieving distributed knowledge on the Grid. The proposed repository can deal with a large variety of different learning contents. Its prototype implementation, developed for Chemistry contents, is part of an extended architecture consisting of a federation of autonomous local repositories. The federation is led by a coordinator who keeps track of the repository in which the learning objects are directly stored or referenced. In each repository server, a locally hosted Web Portal allows a easy management of the repository through a CMS front-end.

Keywords: Chemistry, repository, learning objects, knowledge, Grid.

1 Introduction

Many scientific areas benefit considerably from a system of storage, identification, localization and reuse of data to avoid the cost and effort of rebuilding the existing information. This is particularly true when dealing with higher education scientific knowledge in which teaching material [1] is often the result of a complex procedure that implies time consuming calculations and sophisticated multimedia rendering as typical of physical sciences, like chemistry, whose objective is the understanding of physical phenomena at microscopic (nanometer) level that cannot be directly observed [2]. Quite often such a knowledge is packed into units which do not only represent consistently a well defined topic but do also bear a specific pedagogical background and embody a significant amount of multimediality and interactivity. The production of these units, commonly called Learning Objects (LO)s and generally defined as "any digital resource that can be reused to support learning"[3], is becoming increasingly easier thanks to instruments like Web 2.0 [4] and other ICT products [5]. This makes the LOs highly autonomous learning resources bearing modularity, availability, reusability and interoperability that are qualities enabling their profitable

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 29–40, 2010.

usage in different contexts. These features clearly justify the significant manpower investments usually required for their production and prompt the assemblage of a system of repositories allowing the sharing of LOs among the members of large communities. A repository, in fact, is an environment of an Enterprise Resource Planning (ERP) [6] information system that uses metabases (the set of relational tables, rules and calculation engines through which metadata are managed). This makes the building of a system of distributed LO repositories exploiting the collaborative use of metadata [7] play a key role in the success of physical sciences teaching and learning. For this reason we have addressed our recent research efforts to the design and the implementation of a collaborative repository of scientific LOs. A key feature of our Grid LOs Repository (G-LOREP) project is its focus on large communities that implies both a complex and a distributed nature of the repository. Accordingly, it is based on the adoption of an efficient mechanism of filing and retrieving distributed information as well as on the exploitation of the innovative features of the European production grid infrastructure EGEE [8].

Accordingly the paper is articulated as follows:

In section 2 a description of the general architecture of the Grid repository is given together with the articulation of the metadata scheme and of the Content Management System (CMS) [9] based repository service, the organization of the learning object and the structure of the federation of repositories.

In section 3 the implementation of a repository specific to the Computational Chemistry (COMPCHEM) [10] Virtual Organization (VO) is discussed by illustrating an exemplifying LO.

In section 4 conclusions are summarized.

2 The G-LOREP Repository

2.1 The General Architecture

The G-LOREP repository architecture is based on a client/server model (see Fig. 1) in which a set of clients use the services offered by a server. The model, implemented as a distributed system, consists of the following components:

- A server bearing a CMS offering the needed repository management activities at backend-level (backup, protection, access control, etc.) and the server providing, through a web portal, various services for clients (up/download on/from a local file system, file management, etc.) at frontend-level.
- A set of clients requiring the services offered by the server.
- A network (the EGEE Grid in our case) allowing clients to use available facilities after authentication.
- A Virtual Organization (COMPCHEM in our case) providing access to remote file systems where some LOs can be stored.

The CMS manages directly the metadata DB creating rules and relational tables using the metadata XML schema. The LO metadata consists of the characteristics and references of the LO resource. References are just a collection of paths to the folder containing the LO files.

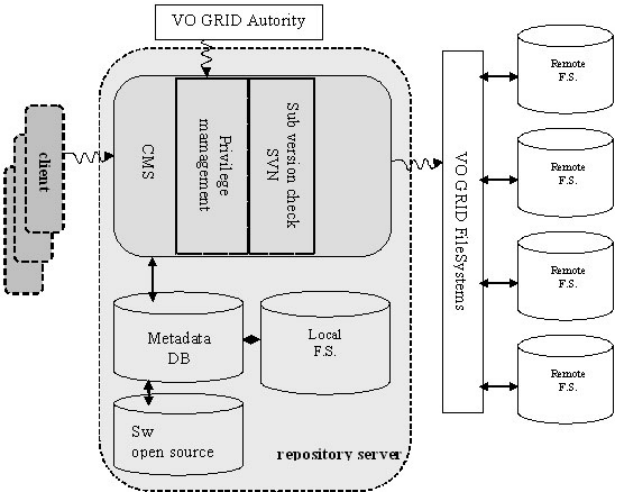


Fig. 1. Architecture of the G-LOREP distributed repository

In the G-LOREP prototype implementation the XML schema [11] representing the metadata connected to the metabase consists of six main elements with attributes. They are illustrated in Fig.2 where the architecture of the XML schema for a metadata is given. As shown by the figure the metadata consists of a Universally Unique Identifier (UUID) [12] that is the standard identifier for each element belonging to the metabase. The other elements are the generaldata (that is the data in itself that consists of title and author), the datatype (that represents the kind of element and could be a digital object or simply a text strictly connected to the generaldata element. It also defines the level of permissions for data access), the searchdata (that represents how the system looks for information in the metabase by searching a keyword in a vocabulary. A vocabulary consists of several keywords listed as terms) and the locationdata (that is the path to the data and its date of creation). A final element is the comment that represents the textfield used by users to comment a previously created element.

In order to cope with the distributed nature of the G-LOREP repository architecture the CMS had to be customized. An open source software package was adopted as an end user supply. An LO set could require a specific software version. The main features that are taken into account are the efficiency in the sharing of a large amount of data without the need to pass them explicitly by a file system to another as well as the need for uniquely locating and identifying the LOs within the Grid network by the Uniform Resource Locator (URL) [13] and the Universally Unique Identifier (URL+ UUID).

2.2 Drupal CMS

As shown in figure 1 to interface the client and to manage the necessary dataset to match the requirements a versatile CMS is needed. For G-LOREP we adopted Drupal

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE repository [
<!ELEMENT repository  (learningobject+)>
<!ELEMENT learningobject (UUID, generaldata, datatype, searchdata, locationdata, comment)>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT generaldata (title, author+)>
                <!ELEMENT title (#PCDATA)>
                <!ATTLIST author
                     surname  CDATA #REQUIRED
                     name  CDATA #REQUIRED
                     email  CDATA #REQUIRED
                     company  CDATA #IMPLIED>
    <!ELEMENT datatype (type,format,version, lang, permissions)>
                <!ELEMENT type (digital, other) (#PCDATA)>
                <!ELEMENT format (#PCDATA)>
                <!ELEMENT version (#PCDATA)>
                <!ELEMENT lang (#PCDATA)>
                <!ELEMENT permissions (anonymous| authenticated| admin)(#PCDATA)>
<!ELEMENT searchdata (vocabulary, description)>
                <!ELEMENT vocabulary (keywords+)>
                  <!ELEMENT keywords (#PCDATA)>
<!ELEMENT description (#PCDATA)>
<!ELEMENT locationdata (creationdate, uridata, flag)>
                <!ATTLIST creationdate
                     year  CDATA #REQUIRED
                     month  CDATA #REQUIRED
                     day  CDATA #REQUIRED
                     time CDATA #REQUIRED>
                <!ATTLIST uridata
                     baseurl  CDATA #REQUIRED
                     path  CDATA #REQUIRED
                     filename  CDATA # REQUIRED >
                <!ELEMENT flag (yes|no) (#PCDATA)>
<!ELEMENT comment (#PCDATA)>
]>
```

Fig. 2. The XML format of our metadata

[14] because of its access rules and administration simplicity as well as for its "non programming skills" capabilities. Drupal is a free and open source CMS written in PHP [15] and distributed under the GNU General Public License. The 6.x release of Drupal includes a "core" containing basic features common to most CMSs. These include the ability to create pages, stories, authentication rules and permissions. Moreover, it allows the adding of several custom features installing "modules" created by the Drupal community members.

Drupal treats most content types as variations of the same concept that is called node (see the central box of Fig. 3). A node could be a page, a digital object (photo, video, etc.), or simply information. With the Content Construction Kit (CCK) module we can create custom contents types for nodes. In our case we specified a content type for VRML projects stored in a File System as compressed archives. Every node is linked to a DB Table containing its ID, title, author, date of creation, type of content, subversion, and has a path to be easily reached.

2.3 Learning Object Repository Server Architecture

Contents can be accessed differently depending on the type of user. We set three types of users with different access rules (administrator, authenticated, anonymous). These rules vary in going from the anonymous user (who cannot access the repository features) to the authenticated user (who is a VO certified user). At top level sits the

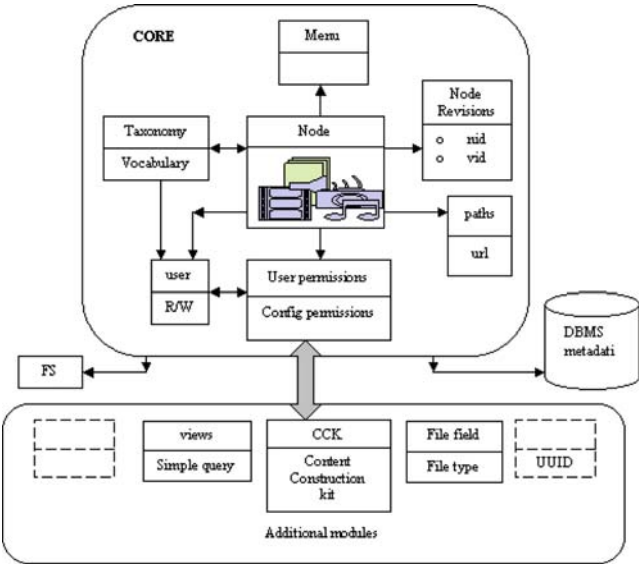


Fig. 3. CMS based repository server

administrator who is responsible for the system management: he/she can create, delete, and edit every kind of settings. Authenticated users can create and upload LOs for each project, whilst they cannot delete them. Site pages access and posting comments are denied to anonymous users. A new user can create his/her personal account on the repository server via a registration form. A "captcha" form has been included to reject computer generated responses.

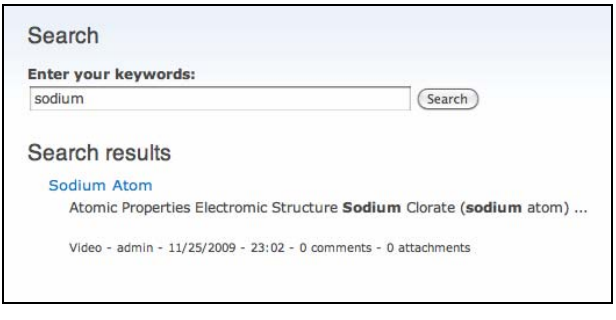


Fig. 4. Search example

Stored projects can be searched using a form located in every page of the main site. This is made possible by the fact that the content is "tagged" in the taxonomy vocabulary and fetched by "views" through an additional module downloadable from the

Drupal community site (see Fig.4). Words appearing in a page are automatically added in a vocabulary in different hierarchies called taxonomies (for example the "sodium atom" term appearing in Fig. 4 belongs to the Chemistry vocabulary). Taxonomy is also accessible via a menu located on the right hand side bar.

2.4 Repositories Federation Architecture

The proposed client/server model could be seen as a small part of a large ecosystem made of many federate repositories. This architecture is a particular example of cloud computing, where many services provide applications that are accessed from a web browser, while the software and data are stored on the servers. Federated repositories cooperate to manage and fetch the LOs using an Index Registry either outside the repositories or inside a leading repository containing references to the federation repositories. The choice of either these two solutions strictly depends on the federation management policy. We chose the second one foreseeing a leading server (see Fig. 5).

Our first prototype is the eligible leading repository server. It can provide a motivation in order to create repositories in other VOs. The proposed communication framework of the whole federation is based on the Really Simple Syndication (RSS) [16] feeds trade. RSS extends the basic XML schema established for more robust syndication of content. The availability of RSS in the Drupal Core supports our choice.

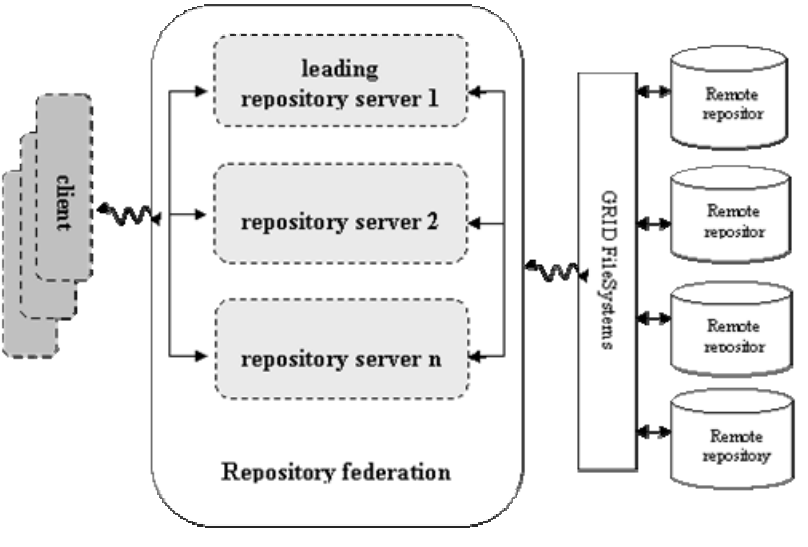


Fig. 5. Repository federation architecture

3 A Repository for Chemistry Learning Objects

As a case study for the practical implementation of G-LOREP we chose the LOs created by the Chemistry component of our research group that is member of the

European Chemistry Thematic Network (ECTN) [17] and has operated in the field of e-learning through the Multimedia Teaching and Learning for Chemistry (MUTALC) working group [18] of ECTN. The Chemistry group of the University of Perugia, as will be described in more detail later on, has produced in recent years some LOs based on the contents of the courses of its Bachelor and Master Chemistry degrees which are fully compliant with the Eurolabel scheme defined by ECTN. To consider some examples among the LOs developed for that purpose we mention here those created to integrate Semantic web approaches and e-learning technologies in a new Learning Management System [19]. Other LOs created as part of the MUTALC activities are those embedded by the group of Oslo in the modules of the General Chemistry and the Organic Chemistry courses, those implemented by the Dresden group in an Analytical Chemistry Laboratory course [20] or by the Technical University of Vienna group in IChemTest [18]. The mention to the above LOs is motivated by the fact that they all are designed to support the preparation of students wishing to undertake self-assessment sessions of the EChemTest [21] electronic tests. This material, however, even when implemented for fruition on the Web, in general is neither structured for a repository nor ready for on line use. Accordingly, in order to make them available on the Grid they had to be properly structured.

3.1 The COMPCHEM VO

The first move made along that direction was, therefore, to collocate them within COMPCHEM. COMPCHEM is the result of a cooperative endeavour of the Department of Chemistry and the Department of Mathematics and Computer Science of the University of Perugia whose aim is to provide a grid environment for molecular knowledge production and handling. COMPCHEM supports several computational chemistry applications providing a shared pool of resources, independent of geographic location, with round-the-clock access to major storage, compute and networking facilities. The EGEE middleware provides a variety of services to the scientists clustered into the various Virtual Organisations. The services range from training and user support, to the maintenance of the software infrastructure necessary to access the resources. Thanks to that, COMPCHEM is willing to offer to its members the possibility of carrying out their teaching and learning activities in chemistry using LOs requiring a substantial amount of computing to support molecular simulations, graphical rendering, semantic handling and numerical treatments. More specifically, the LOs developed within COMPCHEM can combine various levels of virtual reality ranging from the nanometer to the meter scale (which go usually under the name of Molecular Virtual Reality (MVR) as opposite to Human Virtual Reality (HVR) [22]).

As a matter of fact COMPCHEM is equipped to provide its members with the possibility of using as LOs the outcomes of any extended computational campaign carried on the grid when one acts at least as a “passive user” of the VO (as sketched in Table 1 the entry level of the COMPCHEM memberships [23] consists, indeed, of a status in which the user can utilize for free all the software made available by the VO).

Table 1. Levels of membership in COMPCHEM

Level	Description
1-Passive user	Utilize SW implemented on the grid by other members
2-Active user	Implement on the grid SW for personal usage
3-Passive SW provider	Make a stable version of the SW implemented on the grid available to other members
4-Active SW provider	Contribute to the concerted and interoperable use of the SW implemented on the grid
5-Passive HW provider	Confer some HW to the VO
6-Active HW provider	Contribute to the operationality of the grid infrastructure

However, the use of the grid does not turn out to be truly advantageous when trying to utilize its storage facilities since grid storage plays almost exclusively the role of providing temporary home to the intermediate results of the calculations. For teaching and learning activities, instead, a more intelligent use of the grid distributed storage as a repository is in order. For this reason it is of fundamental importance (as already pointed out in the previous section) the fact that COMPCHEM users can build an LO repository by evolving at least to level 2 (see again Table 1).

3.2 The EChemTest Repository

As already mentioned, the key reason for building within ECTN a repository application like G-LOREP was to provide a proper learning support to the self-asessment electronic tests of EChemTest. EChemTest is aimed at evaluating Chemistry knowledge and skills for various purposes. It provides, for example, a useful means to professional workers seeking for career development and industrial mobility, to students seeking for European Academic Exchange and citizens pursuing life-long learning. Therefore the LOs developed for it need not to be targeted to a single category of users. EChemTest is a one hour test made of up to 30 questions of different types, taken at random from a large question bank, covering the Euro-Curriculum Chemistry Program (ECCP) at four different levels. These are equivalent to the Pre-University Level 1 (a person at the end of compulsory education), Pre-University Level 2 (a person at the beginning of University studies), University Bachelor Level 3 (a person at the end of the Core Chemistry Syllabus in agreement with the «Chemistry Eurobachelor®» requirements and University Master Level 4 (a person at the end of a Master degree in one of the specialized chemistry area in agreement with the «Chemistry Euromaster®» requirements). At Level 3 four sets of Libraries have been created (Organic, Inorganic, Physical and Analytical). At Level 4 more specialized (research oriented) libraries have been created. In particular at this level the libraries of Cultural Heritage and Computational Chemistry (CC4) have been developed. Because of the hybrid Computer science and Chemistry composition of our research group the work for implementing the repository was concentrated on CC4 and, in particular on an LO combining HVR and MVR.

3.3 The Virtual Laboratory Experiment

According to the above mentioned reasons, the study case selected in this paper is centered on a chemistry virtual laboratory LO designed using a window on the world approach [24] related to an actual laboratory experiment carried out by our students [25]. Although our virtual laboratory experimentation is being carried out on four study cases (laser-refractometry, liquid surface tension measurements, gas-mass experiments, distillation apparatus assemblage) we shall concentrate in the followings on the gas mass one.

A screen shot of the HVR animation of the gas mass experiment is shown in Fig. 6. In that virtual experiment students can at the same time interact with a computer simulated environment (regardless of whether the simulated environment refers to the real world or to the imaginary world of atoms and molecules). Users can interact with the simulated environment through standard input devices of the traditional type (such as a keyboard and a mouse) or through multimodal devices (such as a wired glove, the Polhemus boom arm and omnidirectional treadmill) [26] even if the whole apparatus is not yet in its final settling.

The code is rendered as virtual simulations using the Virtual Reality Markup Language (VRML) [27]. VRML represents 3-dimensional (3D) interactive vector graphics designed particularly with the World Wide Web in mind. VRML is a text file format where, for example, vertices and edges for a 3D polygon can be specified along with the surface color, UV mapped, textures, transparency, and so on. URLs can be associated with graphical components so that a web browser may fetch a web-page or a new VRML file from the Internet when the user clicks on the specific graphical component. Animations, sounds, lighting, and other aspects of the virtual word can interact with the user or may be triggered by external events such as timers. A special Script Node allows the addition of program code (e.g., written in Java or JavaScript (ECMAScript)) to a VRML file. VRML files are commonly called "worlds" and have the *.wrl extension. Although VRML worlds use a text format, they may often be compressed using gzip so that they transfer over the internet more quickly (some gzip compressed files use the *.wrz extension). Many 3D modeling programs can save objects and scenes in VRML format.

For the gas mass virtual experiment a XML table of materials has been created. XML allow to store information on materials that help implementing the experiment, which may include any material by specifying its name, as the index of refraction, and possibly a color to show its virtual representation (see Fig.6). Simulations for different materials can be therefore implemented at the same time. The nanometer world is treated in a similar fashion and is represented as well in a virtual reality form to provide molecular understanding of the involved chemical structures and processes.

3.4 Performance Issues

Since G-LOREP has been designed mainly for contributors inexperienced in grid computing, performance issues have been at the moment more considered in terms of user (teachers and students) friendliness especially when dealing with unconventional material leveraging on our past work in virtual reality applications for molecular

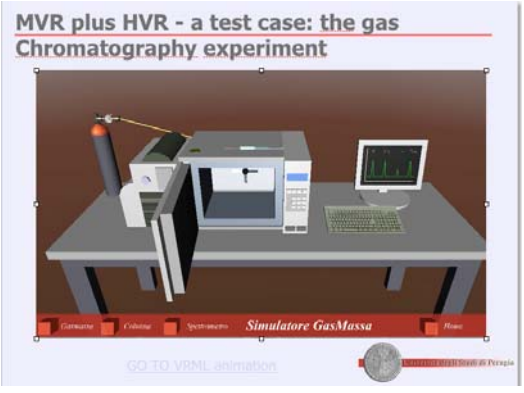


Fig. 6. Gas mass virtual experiment

sciences. As to time, performances are strictly related to those of Apache and Mysql on the used server machine that is a workstation with standard configuration based on a dual-core processor. Preliminary tests were carried on a small Grid area similar to a MAN (Metropolitan Area Network), serving few concurrent users. Moreover the prototype has been working on standard data provided by the Chemistry Department and the Computer Science Department of the University of Perugia. Therefore, even if the G-LOREP prototype is providing effective and efficient response to our current usage, no meaningful comparison can be made at present with other products. The crucial efficiency targeted tests for G-LOREP will come only from its application to the activities of the virtual campus working group (WG5) of the Life Long Learning, Erasmus DG EAC/31/08 (Networks - Academic Networks - European Chemistry and Chemical Engineering Education Network) project as well to the development of the electronic material in Cultural heritage conservation technologies for the 502271-LLP-1-2009-1-GR-ERASMUS-ECDSP projects of which G-LOREP is meant to represent a working tool. As a matter of fact, these two projects will represent not only the G-LOREP test field but also the driving force of its future evolution.

4 Conclusions

Progress in the establishing e-learning procedures in Chemistry is part of the activities of the ECTN thematic network that has already produced standards for teaching and learning labels as well as for self assessment tools. To support these activities our research group has already produced some LOs. The present paper reports on the next important step of developing a systematic approach to the management of the LOs consisting in the design and implementation of a new distributed repository exploiting the innovative features of the computing grids. In the paper we describe in detail the characteristics of this repository and the software environment in which it is based. At the same time we illustrate the articulation of a typical teaching unit.

In summary, on the computer science side the most important achievements of our efforts are the combined exploitation of the repository architecture for distributed

elaboration while on the chemistry side the most important achievements are the structuring of large amounts of chemical knowledge for an open and distance teaching and learning activity.

The perspective result from the combination of the two advances is the potentially straightforward reusability of the large amount of chemistry LOs produced locally by the members of ECTN and other similar organizations.

Acknowledgements

The authors acknowledge financial support from the European project EGEE III, the ESA ESTEC contract 21790/08/NL/HE, the COST CMST European initiatives (Action D37 "GRIDCHEM"), MIUR, and ARPA.

References

1. Falcinelli, E., Gori, C., Jasso, J., Milani, A., Pallottelli, S.: E-studium: blended e-learning for university education support. International Journal of Learning Technology 4(1/2), 110–124 (2009)
2. Laganà, A., Manuali, C., Faginas Lago, N., Gervasi, O., Crocchianti, S., Riganelli, A., Schanze, S.: From Computer Assisted to Grid Empowered Teaching and Learning Activities in Higher Level Chemistry Education. In: Eilks, I., Byers, B. (eds.) Innovative Methods of Teaching and Learning Chemistry in Higher Education. RCS Publishing (2009)
3. Wiley, D.A.: Connecting Learning Objects to Instructional Design Theory: A Definition, A Metaphor, and A Taxonomy. In: Wiley, D.A. (DOC) The Instructional Use of Learning Objects: Online Version (2000), http://reusability.org/read/chapters/wiley.doc
4. Stephens, M., Collins, M.: Web 2.0, Library 2.0, and the Hyperlinked Library. Serials Review 33(4), 253–256 (2007)
5. Regueras, L.M., Verdu, E., Perez, M.A., De Castro, J.P., Verdu, M.J.: An applied project of ICT-based active learning for the new model of university education. Int. J. of Continuing Engineering Education and Life-Long Learning 17(6), 447–460 (2007)
6. Ng, P., Gable, C., Guy, G., Taizan, C.: An ERP-client benefit-oriented maintenance taxonomy. Journal of Systems and Software 64(2), 87–109 (2002)
7. Schweik, C.M., Stepanov, A., Grove, J.M.: The open research system: a web-based metadata and data repository for collaborative research. Computers and Electronics in Agriculture 47(3), 221–242 (2005)
8. EGEE (Enabling Grids for E-Science in Europe), `http://public.eu-egee.org` (accessed November 2009)
9. Content Management System, `http://en.wikipedia.org/wiki/Content_management_system` (accessed November 2009)
10. COMPCHEM, `http://compchem.unipg.it` (accessed November 2009)
11. Tecnology, X.M.L., `http://www.w3.org/standards/xml/` (accessed November 2009)
12. Universally Unique Identifier: MySQL 5.0 Reference Manual, `http://dev.mysql.com/doc/refman/5.0/en/miscellaneous-functions.html#function_uuid` (accessed November 2009)
13. URL, URIs and URNs: Clarifications and Recomandations 1.0, `http://www.w3.org/TR/uri-clarification/` (accessed November 2009)

14. Drupal Documentation, http://drupal.org/handbooks (accessed November 2009)
15. PHP: Hypertext Preprocessor, PHP Manual, http://www.php.net/manual/en/ (accessed November 2009)
16. RSS 2.0 Specification, http://www.w3.org/RDF/, http://validator.w3.org/feed/docs/rss2.html (accessed November 2009)
17. ECTN Network: General Chemistry and the Organic Chemistry courses, http://ectn-assoc.cpe.fr/network/index.htm (accessed November 2009)
18. Lagana', A., Riganelli, A., Gervasi, O., Yates, P., Wahala, K., Salzer, R., Varella, E., Froehlich, J.: ICCSA 2005. LNCS, vol. 3482, pp. 938–946. Springer, Heidelberg (2005)
19. Lagana', A., Riganelli, A., Gervasi, O.: A learning management system based on virtual reality and semantic web techniques in Chemistry studies in the European higher education area. In: Salzer, R., Mitchell, T., Muller-Solger, H. (eds.) Gesellschaft Deutscher Chemiker, p. 105 (2005)
20. Zimmerer, C., Thiele, S., Krauseneck, A., Korndle, H., Salzer, R.: Internet Teaching: laboratory course in Analytical Chemistry. Microchimica Acta 142, 153–159 (2003)
21. EChemTest, http://ectn-assoc.cpe.fr/echemtest/default.htm (accessed November 2009)
22. Gervasi, O., Lagana', A.: Simbex a Portal for the a priori simulation of crossed beam experiments. Future Generation Computer Systems 20, 703–715 (2004)
23. Lagana', A., Riganelli, A., Gervasi, O.: On the structuring of the computational chemistry virtual organization COMPCHEM. In: Gavrilova, M.L., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganá, A., Mun, Y., Choo, H. (eds.) ICCSA 2006. LNCS, vol. 3980, pp. 665–674. Springer, Heidelberg (2006)
24. Gervasi, O., Riganelli, A., Lagana', A.: Virtual reality applied to molecular sciences. In: Laganá, A., Gavrilova, M.L., Kumar, V., Mun, Y., Tan, C.J.K., Gervasi, O. (eds.) ICCSA 2004. LNCS, vol. 3044, pp. 827–836. Springer, Heidelberg (2004)
25. Gervasi, O., Tasso, S., Lagana', A.: Immersive Molecular Virtual Reality based on X3D and Web services. In: Gavrilova, M.L., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganá, A., Mun, Y., Choo, H. (eds.) ICCSA 2006. LNCS, vol. 3980, pp. 212–221. Springer, Heidelberg (2006)
26. Gervasi, O., Riganelli, A., Pacifici, L., Lagana', A.: VMSLab-G: A Virtual Laboratory prototype for Molecular Science on the Grid. Future generation Computer Systems 20(5), 717–726 (2004)
27. VRML Virtual Reality Modeling Language, http://www.w3.org/MarkUp/VRML/ (accessed November 2009)

Porting of GROMACS Package into the Grid Environment: Testing of a New Distribution Strategy

Alessandro Costantini[1,2], Eduardo Gutierrez[3], Javier Lopez Cacheiro[3], Aurelio Rodriguez[3], Osvaldo Gervasi[2], and Antonio Laganà[1]

[1] Department of Chemistry, University of Perugia, Perugia, Italy
[2] Department of Math. and Computer Science, University of Perugia, Perugia, Italy
[3] CESGA, Santiago de Compostela, Spain

Abstract. The paper describes the application porting process onto the EGEE grid of GROMACS package that was carried out using the P-GRADE Grid Portal tool implemented in COMPCHEM. For this purpose a new stategy to access local and distributed resources has been designed and a set of visualization tools has been implemented in order to help chemical insight.

1 Introduction

The increasing availability of computer power on Grid platforms is a strong incentive to implement complex computational suites of codes on distributed systems and to develop appropriate distribution models. This is indeed one of the tasks of the virtual organization (VO) COMPCHEM [1] operating on the production infrastructure of the EGEE Grid [2]. At the same time the QDYN and ELAMS working groups of the COST Action D37 [3] pursue the goal of designing user friendly Grid empowered versions of the workflows [4] for the simulation of molecular systems.

On this ground QDYN and ELAMS working groups have worked jointly on the porting of the Molecular Dynamics package GROMACS [5] on the EGEE Grid in the perspective of offering a widely used molecular simulation tool to COMPCHEM VO members and developing suitable visualization tools to facilitate the comprehension of simulation's outcomes.

GROMACS is, in fact, a suite of programs designed for the simulation of complex systems by making use of a wide variety of Molecular Dynamics techniques. The actual application porting has been carried out using the P-GRADE Grid Portal [6,7]. This open source tool has been chosen because it provides intuitive graphical interfaces for the porting and does not necessarily require the modification of the original code for its distributed execution on a Grid platform.

However, although significant work about integrating computational applications in scientific gateways has been already carried out, not much effort has been spent to the end of achieving their easy and efficient execution across different computing platforms. In particular, while most of the High Throughput

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 41–52, 2010.

(HT) computing resources are available on the Grid, High Performance (HP) platforms (of both the Super Computer or cluster type based on high speed dedicated networks) are only available at large scale facilities. Moreover access to external services (ES) as proprietary databases, applications or Webservers is rarely performed from HT or HP resources. This has motivated us to develop a new distribution strategy and structure a workflow in which the execution is distributed using different computing environments: while the main tasks are executed on the Grid, some tasks are executed on a local cluster and other tasks require the access to a proprietary database.

In this paper, by exploiting the potentialities of the new workflow developed at CESGA (see Ref. [8]) a new alternative strategy for using external services and proprietary applications in COMPCHEM VO is proposed. These enhancements enable the final user to perform complex simulations by combining different softwares and using the output obtained by proprietary applications or stored in private databases as input for CPU demanding applications running on the Grid.

In section 2 the Gridification of the GROMACS package and its implementation on the P-GRADE Grid Portal is described; in section 3 the articulation of the adopted workflow and its measured performances are described; in section 4 the Grid enabled visualization tool implemented on the P-GRADE Grid portal and the new strategy implemented for the distribution are illustrated and analysed. Our conclusions are summarised in section 5.

2 Porting the GROMACS Package to the Grid

2.1 GROMACS Program Overview

Our work has focused on GROMACS because it is a versatile package performing Molecular Dynamics calculations for hundreds to millions of particles. GROMACS is primarily designed for biochemical molecules like proteins and lipids exibiting complicated patterns of bonded interactions. However, since GROMACS is extremely fast also at calculating the nonbonded interactions (which usually dominate molecular simulations) it is also used by several research groups to deal with non-biological systems like polymers.

GROMACS has shown to perform well on scalar machines and scale up satisfactorily with the number of processors on parallel machines. As a matter of fact GROMACS showed to encompass a minimal-communication domain decomposition algorithm, full dynamic load balancing, a state-of-the-art parallel constraint solver, and efficient virtual site algorithms which allow the removal of the hydrogen atom degrees of freedom to accept integration time steps as high as 5 *fs* for atomistic simulations. To improve the scaling properties of the common particle mesh Ewald electrostatics algorithms a Multiple-Program, Multiple-Data approach has been used with separate node domains responsible for direct and reciprocal space interactions [9]. Not only does this combination of algorithms enable extremely long simulations of large systems but it also leads to similar simulation performances on modest numbers of standard cluster nodes.

For all these reasons we have decided to carry out the testing of the cooperative use of the computational resources of the EGEE Grid infrastructure on GROMACS. In our case, as will be discussed in greater detail later on, the bench case study was concerned with the tutorial on the dependence on the temperature of the energy minimization of water solutions.

2.2 The Distribution Workflow

In order to execute the scalar version of GROMACS on multiple Grid resources with different input files simultaneously (the so called "parameter study" modality [10]) we developed a distributed version of GROMACS for the Grid. As these simulations can also run independently from each other they can be distributed on a large numbers of computers. However, to make the execution fault tolerant (Grid resources are more exposed to faults than supercomputers) we need a Grid-specific component able to manage the execution of these jobs, collect Grid resources, transfer the code with the corresponding input files to the computing elements, start the jobs, observe and supervise their execution and finally even stage out the result files after successful completion.

The tool used in our work to gridify GROMACS package was the P-GRADE Grid Portal [6]. P-GRADE provides graphical tools and services which help Grid application developers to port legacy programs onto the Grid without reengineering or modifying them.

P-GRADE has the generical structure of a workflow that enables application developers to define the above mentioned parameter study by means of a graphical environment and to generate out of the user specified description the Grid scripts and commands allowing the execution of the various computational tasks on the distributed Grid platform.

Workflows integrate batch programs into a directed acyclic graph by connecting them together with file channels. A batch program can be any executable code which is binary compatible with the underlying Grid resources, which in our case are typically the gLite middleware [11] and a subset of the EGEE processors. The file channel defines directed data flows between two batch components like the output file of the source program used as input file of the target program, a dependence that the workflow manager subsystem of P-GRADE resolves during the execution of the workflow by transferring and renaming files. After the user has defined the structure of the workflow and has provided executable components for the workflow nodes it has to be described, whether to execute the workflow with just one input data set, or with multiple input data sets in a parameter study fashion. If the latter option is chosen then the workflow manager system of P-GRADE creates multiple instances (one for each input data set) and executes the workflow instances simultaneously.

The Portal server acts as a central component to instantiate workflows, manage their execution and perform the file staging which involves input and output processes. Moreover, the P-GRADE also provides tools to generate input data sets for parameter study workflows automatically. The user has the possibility of attaching the so called "Generator" components to the workflow in order to

create the parameter input files. The workflow manager subsystem executes first the generator(s) and then the rest of the workflow, ensuring that each workflow accesses and processes correct and different permutations of the data files.

3 The Benchmark Test

3.1 The Workflow Articulation

In order to test the workflow developed for GROMACS we used as a case study the one described on the GROMACS tutorials [12] concerning the "Water: Energy minimization of the solvated system". In this case study the different jobs work with different "Temperature" for "LANGEVIN DYNAMICS OPTIONS" values in a typical scaling temperature technique.

For this reason the values of the `bd-temp` (see Table 1) temperatures considered are stored in the same input file as the other input parameters of the simulation. Before the central component can start running the GROMACS jobs, other components need to generate all the necessary input files to be used as input during file stageing to Grid resources.

Accordingly, the central component of the workflow (Labelled as GROMACS SEQ as evidenced by the appearance in the left hand side in the overlapped windows of Fig. 1) is made of a bash script in which the following steps are performed:

- download of the GROMACS executable from a COMPCHEM server;
- configuration of the enviroment variables;
- execution of the GROMACS executable (already compiled on the User Interface machine of the EGEE Grid).

The smaller boxes attached to the component represent the input and output files which are used and produced by the application. During Grid execution the P-GRADE workflow manager is responsible for preparing these files for the Fortran program and transferring them to the EGEE Computing Element. This makes the executable know nothing about the Grid and no modification is required.

The first workflow component is an Automatic Generator (see the GROMACS A_GEN box of Fig. 1). The automatic Generator is a special job type in P-GRADE used to generate input text file variations for the GROMACS job. Using the parameter definition window of the Automatic Generator the Temperature `bd-temp` values have been defined for the bench concurrent simulation (see the right hand side subwindow of Fig. 1). As the parameter definition window of P-GRADE is highly flexible, we could reuse a generic input file of GROMACS and put a parameter key (say p_1 as in the figure) into it. This parameter key is automatically replaced by the actual parameter values during the execution of the workflow to generate the input files before the GROMACS simulation jobs are started.

The third component of the workflow is a Collector job (see the GROMACS COLL box of Fig. 1) which is again a special job type in P-GRADE. A Collector

Table 1. Main input parameters used for the water benchmark calculation of GROMACS

Parameter	Explanation
; RUN CONTROL PARAMETERS	
`integrator` = md	Integrator
`tinit` = 0	Start time in ps
`dt` = 0.002	Timestep in ps
`nsteps` = 10000	Number of steps
`init_step` = 0	Initial step
`comm-mode` = Linear	Mode for center of mass motion removal
`nstcomm` = 1	Number of steps for center of mass motion removal
; LANGEVIN DYNAMICS OPTIONS	
`bd-temp` = 300	Temperature
`bd-fric` = 0	Friction coefficient (amu/ps)
`ld-seed` = 1993	Random seed
; ENERGY MINIMIZATION OPTIONS	
`emtol` = 100	Force tolerance
`emstep` = 0.01	Initial step-size
`niter` = 20	Max number of iterations in relax_shells
`fcstep` = 0	Step size (1/ps^2) for minimization of flexible constraints
...	

in a P-GRADE workflow is responsible for collecting the results of the parameter study workflow, analyzing them and creating a typical user friendly filtered result (to be considered as the final result of the simulation). In our case the Collector simply collects the results from the GROMACS jobs and compresses the files into a single archive file that can be downloaded by the user through the Portal web interface. The purpose of this step is, in fact, to make the results of the computations accessible by the end users.

3.2 The Performances

The gridified version of the GROMACS was made execute the input generator and the GROMACS code simultaneously on multiple Grid resources. GROMACS was compiled in a static way using the standard gnu compiler gcc/g77 and the open source atlas library. Static compilation of the package ensures that the program is binary compatible with the used Computing Elements of the EGEE Grid and that the program will not run into incompatibility errors associated with the usage of dinamically loaded libraries. As we did not modify the code any performance improvement can be ascribed only to the Grid implementation that means to the possibility of running the package for different sets of parameters during the same time window on the resources of the COMPCHEM VO.

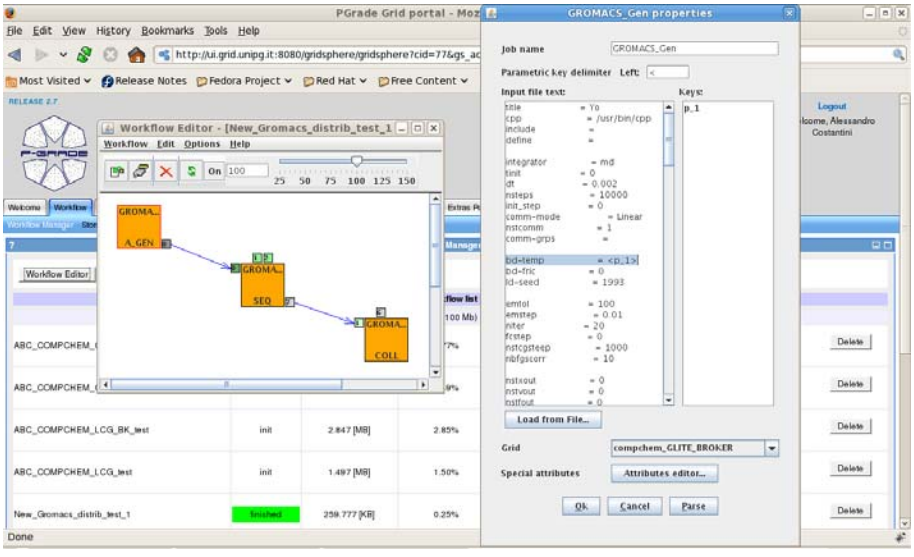


Fig. 1. A schetch of the workflow developed for GROMACS package

COMPCHEM relies on more than 8000 CPUs located at more than 25 European research institutes and universities with most of them not entirely devoted to the COMPCHEM VO since they are shared among several VOs. As a consequence jobs sent by COMPHEM members to these Grid resources compete for CPUs not only with other jobs of COMPCHEM, but also with jobs of other VOs.

As a matter of fact a run of 4 GROMACS jobs in a parameter study fashion for the already mentioned benchmark case took the average time of 100 minutes when using 3 CPUs while the average time taken on 6, 12 and 24 CPUs is 91, 113 and 171 minutes respectively. This allow us to extrapolate an average single CPU time of 33, 15, 9 and 7 minutes respectively. This means that the distribution of GROMACS on the Grid leads to a definite reduction of the average single CPU time if the parameter space is larger than 3.

As the execution time of both the generator and the collector stages are neglegible compared with that of the executor, we can assume that the figures of time consumption quoted above coincide with those of the application as such.

This means that a GROMACS job can spend on the average as much time in the job queue of a single CPU of a Grid resource as on the CPU itself. This obviously means that the average execution time of a job on the Grid is about twice as long as that on a dedicated local machine or that the Grid execution adds about 2-8 hours to each job. Accordingly, as soon as there are at least more than 3 GROMACS jobs running concurrently in a simulation, the Grid based execution takes less time.

4 Further New Features of the Workflow

4.1 Grid Enabled Visualization Tool

As described in Ref. [8] the use of portlets allows to easily add new tabs and windows associated with simulation applications needed by the user. In order to visualize the output coming from the execution of GROMACS workflow, a specific portlet has been developed and implemented in the P-GRAGE Grid Portal under COMPCHEM VO. As P-GRADE is entirely developed using Java [13], JSP [13] and GridSphere [14], these three components were used to develop a specific portlet for the visualization of the GROMACS output.

For this purpose two code files (written using JSP and Java, respectively) and the corresponding configuration files have been developed together with a Jakarta Ant [15] script to deploy the portlet in P-GRADE. At the same time the Jmol package [16] was used as specialized visualization tool. Jmol is an open-source Java viewer for chemical structures which contains a web browser applet (JmolApplet) that can be integrated into web pages or, as in our case, into a GridSphere Portlet. Jmol supports several input file formats, but does not support those of GROMACS. As a solution for that problem the `pdb2gmx` command, integrated in GROMACS package, is used to convert the GROMACS output to Protein Data Bank (PDB) file format [17]. All the described components are packed together in a single tar file for an easy distribution.

In Fig. 2 a screenshot coming from the visualization Jmol portlet implemented in COMPCHEM P-GRADE Grid Portal is shown. Using this portlet the PDB file obtained from the calculations can be easily visualized and there is no need to wait for the completion of the whole workflow. All the functionalities available at the JmolApplet are also present in the portlet. Even more, Jmol additional functionalities like the RasMol/Chime scripting language and JavaScript support library can be integrated in the portlet making the development of a very specific visualization portlet of great help in a specific simulation.

4.2 A New Distribution Scheme

A new workflow (originally designed by CESGA for the G-Fluxo Project [18]) has been implemented and tested also for GROMACS. This specific GROMACS workflow is made up of a chain of three jobs. Each job runs on different platforms (local cluster, CESGA SVG, a laptop and the EGEE Grid infrastructure) as described in Fig. 3. A detailed description of all the features and modifications implemented on P-GRADE can be found in Ref. [8]. This workflow takes advantage of some extra functionalities added to the P-GRADE Grid Portal and in particular:

- File Management and Communication via SSH protocol between different platforms taking into account the dependencies coming from the workflow definition;

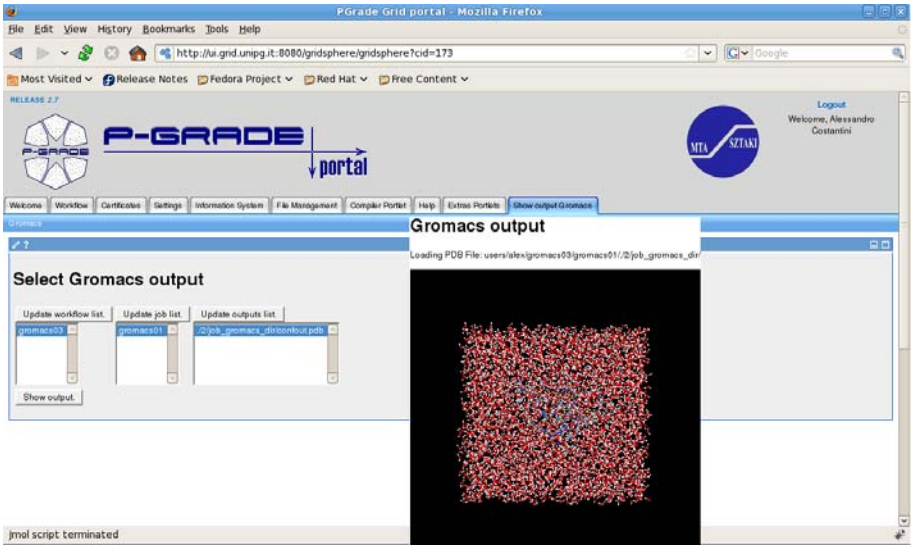


Fig. 2. Output visualization of the developed workflow for GROMACS package

- Job Submission and Monitoring using DRMAA implementation included in the Distributed Resource Management Systems (DRMS) in order to use local resources;
- External services called via web making use of the POST/GET html protocol.

It makes use of the following common tools and applications to perform accurate simulations (see Fig. 4). A schematic representation of the workflow assembled for the study reported in the present paper is illustrated:

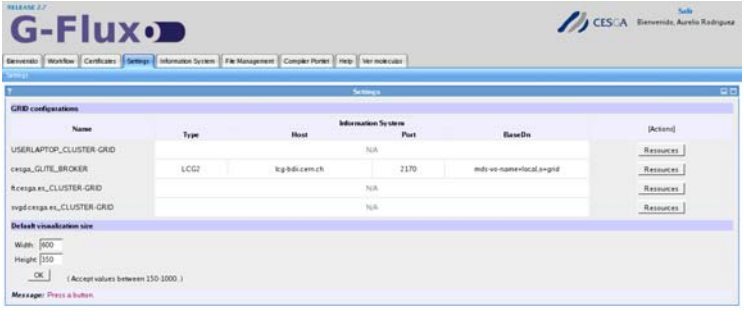


Fig. 3. P-GRADE Grid Portal Grid definitions: EGEE Grid (cesga_GLITE_BROKER), a cluster platform (svgd.cesga.es_CLUSTER-GRID) and an user computer (USER-LAPTOP_CLUSTER-GRID)

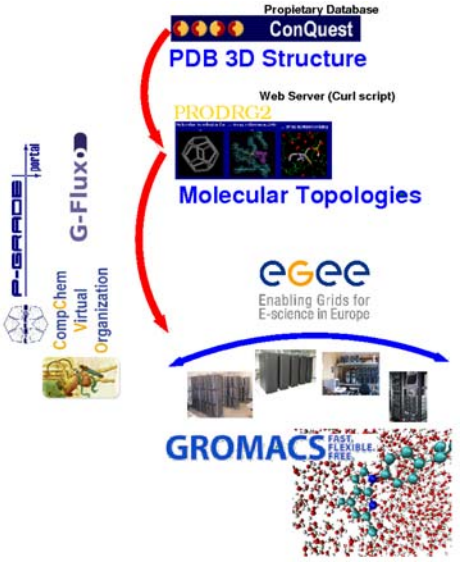


Fig. 4. A schema representing the tools and the execution of the workflow proposed

1. CSD (Cambridge Structural Database [19]): the CSD is accessed through a CESGA server (SVG). This job runs ConQuest in batch mode through the command "cqbatch". A simple query is performed looking for compounds whose name includes the term "azaindole" included. As a result a compressed file (azaindole.tgz) in which all the structural 3D information in form of PDB files coming from the previous query are stored, is returned.
2. PRODRG: This job takes as input the azaindole.tgz file and runs a curl [20] script to make use of an external web server, the Dundee PRODRG2 Server [21] that provides molecular topologies for X-ray refinement/MD and drug design/docking. This job runs from the laptop connected to internet and configured as a CLUSTER-GRID accessible by ssh. As a result a compressed file called azaindole-prodrg.tar, containing the GROMACS ITP files [22] for all the compounds coming from the CSD query, is created.
3. GROMACS: This job runs an energy minimization for every structure made of a box of 1000 water molecules using as input the files contained in the azaindole-prodrg.tar file. It can be easily tuned to run a minimization of the compound with a protein structure (as it is usually performed in protein-ligand complexes studies) relevant to drug design. All the results are stored in a compressed file directly downloadable from the portal.

The workflow used is shown in Fig. 5 and its definition is given in Fig. 6. Relationships between jobs are expressed using a link (this involves a file transfer in each case) that defines the dependency job chain. In this case the user must set all the job ports by following the syntax described in Ref. [8] and taking into

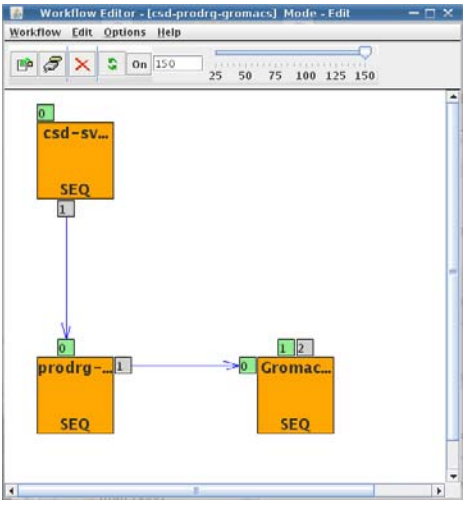


Fig. 5. Workflow Schema as it is presented by the P-GRADE Grid Portal workflow editor

Fig. 6. Workflow definition involving a coordinated execution using Grid (cesga_GLITE_BROKER), Cluster platforms (svgd.cesga.es_CLUSTER-GRID) and a user computer (USERLAPTOP_CLUSTER-GRID)

account where the job is executed so that the portal could be aware of all the information needed for file transfers. In the case of the GROMACS job (to be executed on EGEE) the file should pass through the portal using the local file feature. This is needed to overcome the limitation present in the P-GRADE File Transfer Management System that does not allow direct file transfer between different platforms (different Grid middlewares following the P-GRADE Grid Portal nomenclature). A modification of P-GRADE could enable the direct file transfer between a CLUSTER-GRID and different Grid middleware.

Another interesting improvement would be the connection of a sequential job to an Automatic Generator directly. At present this step need to be performed separately by the user. As a future work, modifications in P-GRADE devoted to overcome this limitation are under study.

5 Conclusions

In the paper the porting procedure of the GROMACS package on the EGEE Grid environment has been described. The GROMACS workflows and Jmol portlet have been successfully implemented in the COMPCHEM computational environment to test the porting of such applications and the performed work is the result of a strong collaboration between the Computational Chemistry Community represented by COMPCHEM VO and the CESGA group. The implemented case study demonstrates not only the power of interdisciplinary group work, but also details the application porting process, providing a reusable example for other groups which are interested in porting applications to production Grid systems. Even if the execution of a single GROMACS job on the Grid is two times slower than that on a local machine, the distribution on the Grid start to be competitive when the parameter space is larger than 3. As an added value we implemented in P-GRADE the visualization tool based on Jmol that enables the user to visualize the output files carried out from the calculations directly in the new portlet. In this paper also a new distribution scheme that facilitates the use of different computational platforms and services in a completely transparent way for the user is presented.

Acknowledgments

Acknowledgments are due for the financial support to COST CMST Action D37 GRIDCHEM, through the activities of QDYN and ELAMS working groups, and EGEE III EU Project under contract IST-2003-508833. Thanks are also due to the Fondazione Cassa di Risparmio of Perugia and Arpa Umbria for the financial support. This work is supported also by Xunta de Galicia under the project G-Fluxo (07SIN001CT). The Grid infrastructures used are those of FORMIGA (07TIC01CT) and EGEE-III (INFSO-RI-222667) projects. Acknowledgments are also due to the Grid Application Supporting Center (GASuC) for help in the use of P-GRADE.

References

1. COMPCHEM, http://compchem.unipg.it
2. EGEE (Enabling Grids for E-Science in Europe), http://public.eu-egee.org
3. QDYN and ELAMS are respectively the working group n. 2 and n. 3 of the CMST COST Action D37, http://www.cost.esf.org/index.php?id=189&action_number=D37
4. Gervasi, O., Laganà, A.: SIMBEX: a Portal for the a priori simulation of crossed beam experiments. Future Generation Computer Systems 20, 703–715 (2004)
5. http://www.gromacs.org
6. P-GRADE Grid Portal, http://portal.p-grade.hu
7. Sipos, G., Kacsuk, P.: Multi-Grid, Multi-User Workflows in the P-GRADE Portal. Journal of Grid Computing 3, 221–238 (2005)

8. Gutiérrez, E., Costantini, A., López Cacheiro, J., Rodríguez, A.: G-FLUXO: A workflow portal specialized in Computational BioChemistry. In: 1st Workshop IWPLS 2009 (2009)
9. Hess, B., Kutzner, C., van der Spoel, D., Lindahl, E.: GROMACS 4: Algorithms for highly efficient, load-balanced, and scalable molecular simulation. J. Chem. Theor. Comp. 4, 435–447 (2008)
10. Thain, D., Tannenbaum, T., Livny, M.: Condor and the Grid in Fran Berman. In: Berman, F., Hey, A.J.G., Fox, G. (eds.) Grid Computing: Making The Global Infrastructure a Reality, pp. 299–336. John Wiley, Chichester (2003)
11. gLite, http://glite.web.cern.ch/glite
12. http://md.chem.rug.nl/education/mdcourse/index.html
13. http://java.sun.com
14. http://www.gridsphere.org/gridsphere/gridsphere
15. http://ant.apache.org
16. http://jmol.sourceforge.net
17. http://www.wwpdb.org
18. http://gfluxo.cesga.es
19. http://www.ccdc.cam.ac.uk/products/csd
20. http://curl.haxx.se
21. http://davapc1.bioch.dundee.ac.uk/prodrg
22. http://www.gromacs.org/Documentation/File_Formats/.itp_File

Hashimoto's Thyroiditis with Petri Nets

Ünal Ufuktepe and Buket Yılmaz

Izmir University of Economics, Department of Mathematics
Balcova, Izmir, Turkey
unal.ufuktepe@ieu.edu.tr

Abstract. Petri Nets (PNs)are promising tool among the various methods for modelling, analyzing and simulating biological systems. This article intents to present the basics of approach and to foster the potential role PNs could play in the development of the computational systems biology.

Hashimoto's Thyroiditis is a type of autoimmune thyroid disease in which the immune system attacks and destroys the thyroid gland. The thyroid helps set the rate of metabolism, which is the rate at which the body uses energy. Hashimotos stops the gland from making enough thyroid hormones for the body to work the way it should. It is the most common thyroid disease in the U.S. we give a PN model for Hashimoto's Thyroiditis.

1 Introduction

Technology provides researchers a huge amount of data necessary. It is important to integrate and organize this data into coherent descriptive models. Such models can shed insight into complex biological processes and suggest new directions for research. The major challenge for the biologist is to integrate and interpret these vast data resources to gain a greater understanding of the structure.

A modeling methodology that is especially tailored for representing and simulating concurrent dynamic systems is Petri Nets (PNs) which have been named after Carl Adam Petri proposed a graphical and mathematical formalism suitable for the modeling and analysis of concurrent, asynchronous, distributed systems [8].

2 Petri Nets

Petri nets are weighted, labeled, directed-bipartite graphs, with tokens that "move around" the graph as reactions take place. There are two types of nodes: places (depicted as circles) and transitions, which are narrow rectangles. Places represent resources of the system while transitions correspond to events to change the state of the resources. Arcs connect places with transitions. Arcs may only be directed from place to transition (in which case they are referred to as input arcs) or transition to place(making them output arcs).

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 53–61, 2010.

A net is $PN = (P, T, F, W, M_0)$ where; $P = \{p_1, p_2, \ldots, p_m\}$ is a finite set of places, $T = \{t_1, t_2, \ldots, t_m\}$ is a finite set of transitions, $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs, W is a weight function of arcs (default = 1), $M_0 : P \to \{0, 1, 2, \ldots\}$ is the initial marking where $P \bigcap T = \varnothing$ and $P \bigcup T \neq \varnothing$. At any time of the evolution of a PN, places hold zero or positive number of tokens. The state of the system is represented by the allocation of tokens over the places and called a marking.

A transition is enabled if its input places contain at least the required numbers of tokens. The firing of an enabled transition will then result in the consumption of the tokens of its input places and the production of a number of tokens in its output places. This represents the dynamical evolution of the system.

A marking M_i is said to be reachable from marking M_j if there is a sequence of transitions that can be fired starting from M_j which results in the marking M_i. A PN is said to be k-bounded if in all reachable marking no place has more than k token. 1-bounded PN is said to be safe.

Reachability is a fundamental basis for studying in the dynamic properties of any system. Deciding, whether a certain marking (sate) is reachable from another marking. A marking M_n is said to be reachable from a marking M_0 if there exists a sequence of firings that transforms M_0 to M_n. A Petri net and it's marking graph are given in Fig.1.

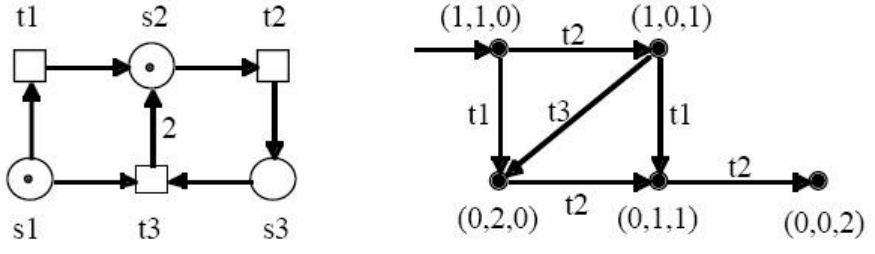


Fig. 1. Marking graph

A PN is deadlock-free if each reachable marking enables a transition. A firing sequence is denoted by $\sigma = M_0 t_1 M_1 t_2 M_2 \ldots t_n M_n$ or simply $\sigma = t_1 t_2 \ldots t_n$. In this case, M_n is reachable from M_0 by σ and we write $M_0[\sigma > M_n$. The set of all possible markings reachable from M_0 in a net (N, M_0) is denoted by $R(N, M_0)$ or simply $R(M_0)$ and the set of all possible firing sequence is denoted by $L(N, M_0)$ or simply $L(M_0)$ [6,7].

3 Biological Applications

Petri nets are a tool for the study of systems. Petri net theory allows a system to be modeled by a Petri net, a mathematical representation of the system. Analysis of the Petri net can then, reveal important information about the structure and

dynamic behavior of the modeled system. Computational models of biological networks will help us deeply understand the development of living organisms. J.Barjis and I.Barjis applied the Petri net modeling technique to model the protein production process [1]. S.Lanzeni et al. showed that Petri Nets are useful in biochemical networks representation and for steady state pathways identification [3].

Understanding how an individual's genetic make-up influences their risk of disease is a problem of paramount importance. Although machine-learning techniques are able to uncover the relationships between genotype and disease, the problem of automatically building the best biochemical model of the relationship has received less attention. J.H.Moore and L.W.Hahn evaluated whether the Petri net approach is capable of identifying biochemical networks that are consistent with disease susceptibility due to higher order nonlinear interactions between tree DNA sequence variations[5,9]. M.Mayo described a method based on random hill climbing that automatically builds Petri net models of non-linear disease-causing gene-gene interactions[4].

4 Hashimoto's Thyroiditis and a Petri Net Model

Hashimoto's Thyroiditis (HT) is a type of autoimmune thyroid disease in which the immune system attacks and destroys the thyroid gland. HT results from a malfunction in the immune system. When working properly, the immune system is designed to protect the body against invaders, such as bacteria, viruses, and other foreign substances. When hypothyroidism is present, the blood levels of thyroid hormones can be measured directly and are usually decreased. However, in early hypothyroidism, the level of thyroid hormones (T3 and T4) may be normal. Therefore, the main tool for the detection of hyperthyroidism is the measurement of the Thyroid-simulating hormone(TSH). If a decrease of thyroid hormone occurs, the pituitary gland reacts by producing more TSH and the blood TSH level increases in an attempt to encourage thyroid hormone production. This increase in TSH can actually precede the fall in thyroid hormones by months or years. Some patients with Hashimoto's Thyroiditis may have no symptoms. However, the common symptoms are fatigue, depression, sensitivity to cold, weight gain, forgetfulness, muscle weakness, puffy face, dry skin and hair, constipation, muscle cramps, and increased menstrual flow. Some patients have major swelling of the thyroid gland in the front of the neck, called goiter.

TSH level in the blood is the most accurate indicator of hypothyroidism. TSH is produced by another gland, the pituitary, which is located in the center of the head behind the nose. The level of TSH rises dramatically when the thyroid gland even slightly underproduces thyroid hormone, so a normal level of TSH reliably excludes hypothyroidism in patients with normal pituitary function. Free T4 (thyroxine) is the active thyroid hormone in the blood. A low level of free T4 values in the normal range may actually represent thyroid hormone deficiency in a particular patient, since a high level of TSH stimulation may keep the free T4 levels within normal limits for many years. Thyroid hormone medication can replace the hormones the thyroid made before the inflammation started.

There are two major thyroid hormones made by a healthy gland (T3 and T4). Replacing one or both of these hormones can alleviate the symptoms caused by the absolute or relative lack of hormones as a consequence of Hashimoto's thyroiditis. Without medication, there is very little chance the thyroid would be able to maintain hormone levels within the normal range, and symptoms and signs of hypothyroidism would occur or worsen. In this paper, we focused on creating a compact models to show the behavior of disease. We used places to show hormones and the organs. Transitions define the connections between the organs and the hormones that are produced by those organs [10].

4.1 Petri Net Model of Healthy Human

In healthy human body, TSH alerts the Thyroid gland, when it gets this alert, it produces thyroid hormones. The rate of T4/T3 should be 13. In the model in Figure 2., the place p_1 sends the TSH to Thyroid gland to make it produces T3 and T4. t_2 defines that the Thyroid gland works well and T3 and T4 are produced efficiently. In healthy human body, T3 is produced by T4 occasionally. The transition t_3 shows the production of T3 by T4. The path from place p_3 to the transition t_6 (p_3, t_5, p_6, t_6) is for the path of Free-T3 in the blood. The path from place p_4 to the transition t_6 (p_4, t_4, p_5, t_6) has the same duty for Free-T4. t_6 sends a message to p_7 (Hypothalamus) that means, the levels of T3 and T4 are normal and Thyroid gland works well. t_7 shows that Hypothalamus is alerted and it produces TRH. t_8 sends a message to p_9 (TRH) from p_8 (PG) and TRH alerts PG to produce TSH. The last transition t_9 sends a message to p_1 from p_9 (Pituiatory Gland) and TSH is produced again. $\{1, 0, 0, 0, 0, 0, 0, 0, 0\}$ is the initial marking. One token is enough for place p_1 to fire the system.

The set of places: (p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9)

p_1 : The TSH hormone.
p_2 : Thyroid gland.
p_3 : Free-Triiodothyronine (T3-Thyroid hormone).
p_4 : Free-Thyroxine (T4-Thyroid hormone).
p_5 : The value of Free-T4 in the blood.
p_6 : The value of Free-T3 in the blood.
p_7 : The Hypothalamus.
p_8 : The TRH hormone.
p_9 : The Pituiatory Gland.

The set of transitions: (t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9)

t_1 : It ensures that TSH can send a message to Thyroid gland to produce thyroid hormones.
t_2 : It produces T3 and T4.
t_3 : T3 is produced by T4.
t_4 : It determines the value of Free-T4 in the blood.
t_5 : It determines the value of Free-T3 in the blood.

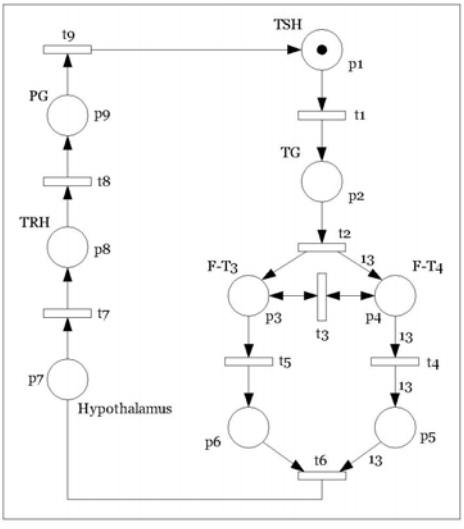


Fig. 2. A Petri net model for healthy human

t_6 : It sends a message to Hypothalamus that the levels of Free-T3 and Free-T4 are normal or not.
t_7 : It sends a message from Hypothalamus to produce TRH.
t_8 : It alerts the Pituiatory Gland to produce TSH.
t_9 : It sends a message from Pituiatory Gland to produce TSH.

4.2 Petri Net Model of Sick Human

This model describes the sick human body system. The reasons of Hashimoto's Thyroiditis are unknown. The human body produces antibodies to thyroid cells cause of these unknown reasons. If there exists these reasons t_1 fires and the place p_2 has tokens (t_1 is a source transition). That means antibodies are produced. Besides of the antibodies p_1 (TSH) tries to alert thyroid gland normally. But, in this model when t_4 gives tokens to p_3, t_3 or t_5 can fire and thyroid gland (TG) loses some of its' tokens because of antibodies. So thyroid gland can not produce T3 and T4 enough. The initial marking is $\{1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}$. At the beginning, one token in p_1 is enough to fire the system. In Hashimoto's Thyroiditis, value of TSH is high while values of T3 and T4 are low. To show that higher TSH value, we used t_2 to explain that if antibodies exist, TG is damaged and value of TSH is high, we give two to the weight of arc between t_2 and p_1.

The set of places: $(p_1,\ p_2,\ p_3,\ p_4,\ p_5,\ p_6,\ p_7,\ p_8,\ p_9,\ p_{10},\ p_{11})$

p_1 : The TSH hormone.
p_2 : Antibodies.
p_3 : The Thyroid gland.
p_4 : Free-Thyroxine (T4-Thyroid hormone).

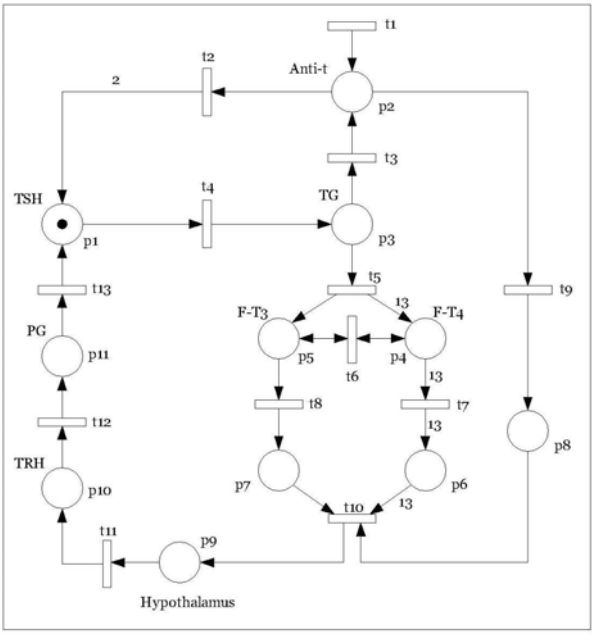


Fig. 3. A Petri net model for sick human

p_5 : Free-Triiodothyronine (T3-Thyroid hormone).
p_6 : The value of Free-T4 in the blood.
p_7 : The value of Free-T3 in the blood.
p_8 : The value of antibodies in the blood.
p_9 : The Hypothalamus.
p_{10} : The TRH hormone.
p_{11} : The Pituiatory Gland.

The set of transitions: $(t_1,\ t_2,\ t_3,\ t_4,\ t_5,\ t_6,\ t_7,\ t_8,\ t_9,\ t_{10},\ t_{11},\ t_{12},\ t_{13})$

t_1 : It defines the unknown reasons and it makes the human body produces antibodies to the thyroid cells.
t_2 : It sends the effects of antibodies and makes the value of TSH high.
t_3 : It defines the damage in the Thyroid gland because of the antibodies.
t_4 : It ensures that TSH can send a message to Thyroid gland to produce thyroid hormones.
t_5 : It produces T3 and T4.
t_6 : T3 is produced by T4.
t_7 : It determines the value of Free-T4 in the blood.
t_8 : It determines the value of Free-T3 in the blood.
t_9 : It sends a message to p_8 that antibodies are produced.
t_{10} : It sends a message to Hypothalamus that the levels of Free-T3 and Free-T4 are normal or not.

t_{11} : It sends a message from Hypothalamus to produce TRH.
t_{12} : It alerts the Pituiatory Gland to produce TSH.
t_{13} : It sends a message from Pituiatory Gland to produce TSH.

4.3 Petri Net Model of Healthy-Sick and on Treatment

This model combines three different situations. System starts with t_1, after t_1 gives a token to p_2 (TG), there are two different firing sequences. One of them is for healthy human. This sequence is almost same with first model in Figure 2. The other firing sequence includes treatment. If t_3 fires, that means; Thyroid gland is damaged and thyroid hormones aren't produced efficiently. For treatment we used place p_5 as a medicine. When t_5 fires, T3 and T4 hormones are taken as a medicine.

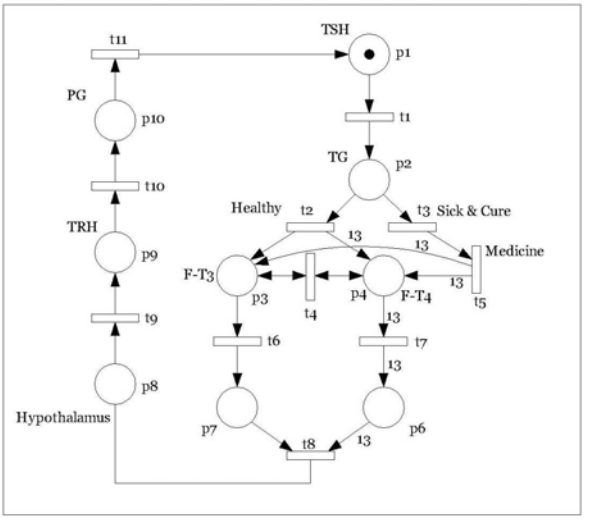


Fig. 4. A Petri net model for healthy-on treatment

The set of places: (p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10})

p_1 : The TSH hormone.
p_2 : The Thyroid gland.
p_3 : Free-Triiodothyronine (T3-Thyroid hormone).
p_4 : Free-Thyroxine (T4-Thyroid hormone).
p_5 : It defines the treatment.
p_6 : The value of Free-T4 in the blood.
p_7 : The value of Free-T3 in the blood.
p_8 : The Hypothalamus.
p_9 : The TRH hormone.
p_{10} : The Pituiatory Gland.

The set of transitions: $(t_1,\ t_2,\ t_3,\ t_4,\ t_5,\ t_6,\ t_7,\ t_8,\ t_9,\ t_{10},\ t_{11})$

t_1 : It ensures that TSH can send a message to Thyroid gland to produce thyroid hormones.
t_2 : It defines that the body works well and TG can produce T3 and T4.
t_3 : It defines the damage in the Thyroid gland because of the antibodies and it sends a message to the treatment place.
t_4 : T3 is produced by T4.
t_5 : It produces T3 and T4.
t_6 : It determines the value of Free-T3 in the blood.
t_7 : It determines the value of Free-T4 in the blood.
t_8 : It sends a message to Hypothalamus that the levels of Free-T3 and Free-T4 are normal or not.
t_9 : It sends a message from Hypothalamus to produce TRH.
t_{10} : It alerts the Pituiatory Gland to produce TSH.
t_{11} : It sends a message from Pituiatory Gland to produce TSH.

We used "Thomas Braunl's S/T Petri-Net Simulation System" and "Luis Alejandro Cortes' SimPRES" to test these models. They can be found at [2] .

5 Conclusion

We used a classical Petri Nets for modeling of basic behavior of Hashimato's Thyroiditis. It is easy to observe the behavior of the disease with initial marking and reachability graph of these models. Timed-colored and Stochastic Petri Nets are more acceptable for having more efficient models for Hashimato's Thyroiditis.In the future study, we will analyze the disease and have efficient results for human body with using detailed Timed-colored Petri Nets models.

References

1. Barjis, J., Barjis, I.: Formalization of the Protein Production by Means of Petri Nets. In: International Conference on Information Intelligence and Systems (ICIIS 1999), p. 4 (1999)
2. INFORMATIK, http://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/java/
3. Lanzeni, S., Messina, E., Archetti, F.: Towards Metobolic networks phylogeny using Petri Nets based expansional analysis. BMC Systems Biology, 17 (2007)
4. Mayo, M.: Learning Petri net models of non-linear gene interactions. BioSystems 82, 74–82 (2005)
5. Moore, H.J., Hahn, W.L.: Petri net modeling of high-order genetic systems using grammatical evolution. BioSystems 72, 177–186 (2003)
6. Murata, T.: Petri Nets: Properties, Analysis and Applications. Proceedings of the IEEE 20(4) (1989)
7. Murata, T.: State equation, controllability, and maximal matchings for Petri nets. IEEE Trans. Automat. Contr. Ac-22(3), 412–416 (1977)

8. Petri, A.C.: Kommunikation mit Automaten. Bonn: Institut für Instrumentelle Mathematik, Schriften des IIM, No.3 (1962); Also,English translation: Communication with Automata, Griffiss Air Force Base, New York. Tech. Rep. RADC-TR. 1(suppl. 1) (1966)
9. Ritchie, M., Hahn, L., Roodi, N., Renee Bailey, L., Dupont, W., Parl, F., Moore, J.: Multifactor-dimensionality reduction reveals high-order interactions among estrogen-metabolism genes in sporadic breast cancer. Am. J. Hum. Genet. (69), 138–147 (2001)
10. Vorherr, H.: Thyroid disease in relation to breast cancer. Journal of Molecular Medicine 56(23), 1139–1145 (1978)

Modelling of the Temporomandibular Joints and the Role of Medical Informatics in Stomatology

Josef Daněk[1,2], Petra Hliňáková[3], Petra Přečková[2,4], Taťjána Dostálová[3,4], Jiří Nedoma[2,3], and Miroslav Nagy[2,4]

[1] Department of Mathematics, University of West Bohemia, Pilsen, Czech Republic
danek@kma.zcu.cz
[2] Institute of Computer Science AS CR. Prague, Czech Republic
nedoma@cs.cas.cz
[3] Charles University, 2nd Medical Faculty, Dept. of Pediatric Stomatology, Prague, Czech Republic
{Petra.Hlinakova,Tatjana.Dostalova}@fnmotol.cz
[4] Centre of Biomedical Informatics, Prague, Czech Republic
{preckova,nagy}@euromise.cz

Abstract. This contribution deals with the 3D analysis of the temporomandibular joint. The main goal is to give the suitable formulation of mathematical model describing with sufficiently accuracy the TMJ and its function. The model is based on the theory of semi-coercive contact problems in linear elasticity, which leads to solving the variational inequality. The numerical solution is based on the finite element approximation of variational inequality corresponding to a generalized semi-coercive contact problem. The obtained numerical results will be discussed. Since the world is globalized new results from the bioinformatics and medical informatics play an important role. Therefore, the problem of an "international global mutual language" for surgeons in stomatology from different countries, and similarly in other branches in medicine, will be shortly discussed.

1 Introduction

The masticatory system is anatomically and functionally complex, with multiple muscle groups with interact to produce forces on a mandible constrained by irregularly shaped joints, articulation (multiple dental contacts) and soft tissues. Human jaw motion is controlled by three pairs of anatomically heterogeneous closing muscles, and at least two pairs of depressors. Active and passive muscle tensions contribute to the jaw's resting posture.

Detailed knowledge about the function and morphology of temporomandibular joint is necessary for clinical applications, and moreover, for analyses of the function of temporomandibular joints and their artificial replacements. Forces are applied to the mandible through the teeth, the muscles of mastication, and through reaction forces at the temporomandibular joint (TMJ). During mastication the chewing muscles generate a masticatory force, which may be up to 4000N. The temporomandibular joint is a bilateral composed joint connecting the mandible

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 62–71, 2010.

to the temporal bone. Both TMJs function bilatarally and any of one side influents the contralateral joint. TMJ has two articular bone components - mandibular condyle and glunoid fossa of the temporal bone. The shape of condyle is the ellipsoid with a mediolateral diameter $\sim$ 20 mm and an anteroposterior diameter $\sim$ 10 mm and the long axis of both condyles form an angle of about 150-160°. Peck et al. (see [10]) provide a typical curvilinear condylar path, the lateral profile of this typical boundary describes by the function of the form $y = 5 \times \cos(x/13 \times \pi) - 5$, where x and y denote the anteroposterior and superinferior co-ordinates, in mm, respectively. The articular surface is covered with the fibrocartilage as the fibrocartilage is more resistant to degenerative changes and it has better regeneration qualities. The jaw at the maximum gape is represented by an interincisal opening of 50 mm and a sagittal-plane rotation of 30° (see [9]). The TMJ disc (discus articularis) is of a biconcave shape that fills the space between articular surfaces thus compensating their incongruities. The disc has a complicated composition, because it functions as a stress absorber and balances irregularities of the shape and the size of anatomical surfaces. The disc is attached to the joint capsule dividing the intracapsular space into upper (discotemporalis) and lower (discomandibular) parts. The disc is often changed by degenerative processes.

The TMJs function symmetrically and this harmony allows biting, chewing and speaking. The synovial fluid is essential for a TMJ function. Movements of TMJ are biomechanically sophisticated and still not clear (see [6]). There are two types of movement: 1. rotary movement, 2. sliding movement. The disc is compressed during the rotary movement and stretched and shortened during the sliding movement.

To fully understand the response of the mandible to forces, we need to know how the internal forces are distributed through the mandible and how the mandible deforms as a consequence of those internal forces. The internal force intensity at a point is characterized by the six independent stress components, and the deformation in the neighbourhood of a point is characterized by the six independent strain components. Therefore, mathematical modelling of movements of the temporomandibular joint (TMJ) and distributions of the stress-strain fields in the TMJ as well as in the TMJP can be used for better understanding of the TMJ and its artificial replacement, biomechanical aspects, its morphology and functions (see [8]). For mathematical models a CT and MRI, with their high resolution ability, like contrast resolutions, serial tomography together with radiography, are used.

2 Mathematical TMJ and TMJP Models

Computer modelling of the TMJ and TMJP and mathematical simulation of their functions are a promising way to study musculoskeletal biomechanics. Computer-generated models have been used to study the mechanics of the muscle function and TMJ forces in humans. Computer models of the craniomandibular apparatus are based on human anatomical features. These models usually represent the mandible as a three-dimensional rigid body, upon which muscle and joint

forces act. The craniomandibular apparatus is mechanically indeterminate because many different combinations of muscle and joint forces can produce static equilibrium for a given load applied to the chin. We distinguish two types of biomechanical models - models, where the TMJ is statically loaded and models, where the TMJ is dynamically loaded.

Models of the temporomandibular joints (TMJs) and their prosthesis (TMJPs) would make clear relationships among the structure and the function. The models of the TMJs and their artificial replacements (TMJP) will be based on the geometry obtained from a computer tomography (CT) and/or of a magnetic resonance imaging (MRI). MRI contrary to CT scan enables simultaneous visualization of all tissues and it is the most preferred imaging technique in many institutions for the study of the TMJ soft tissue pathology. The natural joint presents a system in equilibrium, where the shape is best suitable for its function. The disbalance will result in failure of function and integrity of TMJ. This equally applies to a prosthesis. Therefore, the goal of the mathematical model of TMJ and TMJ prosthesis (TMJP) functions is to establish conditions for preventing the disbalance of the harmony and/or potential destruction of TMJ and TMJP. TMJ is strained by traction and pressure. Contact surfaces tend to separate traction or press together. The effect of the traction power is contained by ligaments, the joint functions as a mobile connection between the mandible and other skeletons, within certain limits (see [5]). In the mathematical representation of our models we speak about a "gap". Contact surfaces are pushed together during the pressure, so the movements between articulating structures happen within a tight connection of sliding articular surfaces.

The synovial fluid is essential for the TMJ function. The synovial fluid contains a glycoprotein lubricin, which serves to lubricate and minimize the friction between the contact surfaces. The friction between contact surfaces causes a waste of the structure and similarly in the case of prostheses. The friction in the sense of the Coulomb law depends on a normal component of the acting force; with increasing of a normal force the friction, deformations and wear are also increasing. The mathematical models have to respect all these facts, enabling us to analyze situations on articulating surfaces.

This used model represents simple approximation of a TMJ and TMJP functions. The aim of this contribution is to present the mathematical model which can be used with sufficient accuracy for stomatogy clinical practice because it corresponds to the real situation in the TMJ and TMJP and according to knowledges and experiences of specialists in stomatology.

2.1 Formulation of the Contact Problem with Given Friction

This contribution deals with the solvability of a generalized semi-coercive contact problem in linear elasticity describing the global model of the joint. Through the contribution the problem will be formulated as the primary variational inequality problem, i.e. in terms of displacements (see [4]). The model includes a mandible, which in the real situation moved three-dimensionally relative to a fixed cranium. We will use a right-handed coordinate system to express geometry, forces

and in the dynamic case also motions. We limit ourselves to the case with the mandible and the skeleton only. The geometry will be based on the MRI data. We will assume the generalized case of bodies of arbitrary shapes which are in mutual contacts. About the skeleton we will assume that it is absolutely rigid. On one part of the boundary the bodies are loaded and on the second one they are fixed, and therefore, as a result, some of the bodies can shift and rotate. Furthermore, we will formulate the model problem in its general form assuming that the body is created by a system of s ($s \geq 2$) bodies being in mutual contacts.

In our study we will assume the case of statically loaded TMJs (TMJPs). Distributions of the stress-strain and displacement fields leads to the following problem (see [5]):

Problem 1. Find a vector function $\mathbf{u}$, satisfying

$$\frac{\partial \tau_{ij}(\mathbf{u}^\iota)}{\partial x_j} + F_i^\iota = 0, \quad i,j = 1,2,3, \quad \text{in } \Omega^\iota, \tag{1}$$

$$e_{ij} = e_{ij}(\mathbf{u}) = \frac{1}{2}\left(\frac{\partial u_i}{\partial x_j} + \frac{\partial u_j}{\partial x_i}\right), \quad i,j = 1,2,3, \tag{2}$$

$$\tau_{ij}^\iota = c_{ijkl}^\iota e_{kl}(\mathbf{u}^\iota), \quad i,j,k,l = 1,2,3, \ \iota = 1,\ldots,s, \tag{3}$$

$$u_n^k(\mathbf{x}) - u_n^l(\mathbf{x}) \leq d^{kl} \quad \text{on} \quad \Gamma_c^{kl}, \tag{4}$$

$$\tau_n^k(\mathbf{x}) = \tau_n^l(\mathbf{x}) \equiv \tau_n^{kl}(\mathbf{x}) \leq 0 \quad \text{on } \Gamma_c^{kl}. \tag{5}$$

$$(u_n^k(\mathbf{x}) - u_n^l(\mathbf{x}) - d^{kl})\tau_n^{kl}(\mathbf{x}) = 0 \quad \text{on } \Gamma_c^{kl}. \tag{6}$$

$$u_i^\iota = u_0^\iota \quad \text{on} \quad \Gamma_u^\iota, \quad \iota = 1,\ldots,s, \tag{7}$$

$$\tau_{ij} n_j = P_i, \quad i,j = 1,2,3 \quad \text{on } \Gamma_\tau, \tag{8}$$

$$u_n = 0, \ \tau_{tj} = 0, \quad j = 1,2,3 \quad \text{on } \Gamma_0. \tag{9}$$

2.2 Variational (Weak) Solution of the Problem

We find a displacement vector $\mathbf{u} = (u_i) \in W \equiv [H^1(\Omega^1)]^3 \times \cdots \times [H^1(\Omega^s)]^3$, where $H^1(\Omega^\iota)$ is the Sobolev space in the usual sense. We assume that $F_i^\iota \in L^2(\Omega^\iota)$, $P_i \in L^2(\Gamma_\tau)$, $u_{0i} \in H^{\frac{1}{2}}(\Gamma_u)$. Let us denote by $(.,.)$ the scalar product in $[L^2(\Omega)]^N$, by $\langle .,. \rangle$ the scalar product in $[L^2(\Gamma_c)]^3$. Let $V = \{\mathbf{v} \,|\, \mathbf{v} \in W, \ \mathbf{v} = \mathbf{u}_0 \text{ on } \Gamma_u, \ v_n = 0 \text{ on } \Gamma_0\}$ be the space of virtual displacements and $K = \{\mathbf{v} \,|\, \mathbf{v} \in V, \ v_n^k - v_n^l \leq d^{kl} \ \text{ on } \cup_{k,l} \Gamma_c^{kl}\}$ be the set of all admissible displacements. Then the problem leads to the following variational inequality:

Problem 2. Find a function $\mathbf{u} \in K$, such that

$$a(\mathbf{u}, \mathbf{v} - \mathbf{u}) + \left\langle g_c^{kl}, \left|\mathbf{v}_t^k - \mathbf{v}_t^l\right| - \left|\mathbf{u}_t^k - \mathbf{u}_t^l\right| \right\rangle \geq S(\mathbf{v} - \mathbf{u}) \quad \forall \mathbf{v} \in K, \tag{10}$$

where for $\mathbf{u}, \mathbf{v} \in W$ we put

$$a(\mathbf{u},\mathbf{v}) = \textstyle\sum_{\iota=1}^s a(\mathbf{u}^\iota, \mathbf{v}^\iota) = \int_\Omega c_{ijkl} e_{ij}(\mathbf{u}) e_{kl}(\mathbf{v})\, d\mathbf{x},$$
$$S(\mathbf{v}) = \textstyle\sum_{\iota=1}^s S^\iota(\mathbf{v}^\iota) = \int_\Omega F_i v_i \, d\mathbf{x} + \int_{\Gamma_\tau} P_i v_i \, ds,$$
$$j_{gn}(\mathbf{v}) = \textstyle\int_{\cup_{k,l} \Gamma_c^{kl}} g_c^{kl} |\mathbf{v}_t^k - \mathbf{v}_t^l| \, ds = \langle g_c^{kl}, |\mathbf{v}_t^k - \mathbf{v}_t^l| \rangle.$$

Numerically the problem will be solved by the finite element technique (see [5]).

3 Numerical Results

The main objective of this contribution is to introduce a three-dimensional finite element model to calculate the static loading of the TMJ and to characterize processes in the TMJ during its function. A model of the mandible was created using the dataset of axial magnetic resonance images (MRI) of a male which was obtained from the Visible Human Project. The finite element mesh (see Fig. 1) was prepared using the Open Inventor 3D toolkit by the Mercury Visualization Sciences Group. The skeleton is assumed to be absolutely rigid. The model data: discretization statistics are characterized by 7295 tetrahedrons and 2043 nodes. The values of material parameters are $E = 1{,}71 \times 10^{10}$[Pa], $\nu = 0{,}25$ for the bone tissue. On the basis of the previous results obtained for the two-dimensional models (see [5]), we set the following boundary conditions presented in (Fig. 1). For the upper side of teeth we assumed a vertical displacement of about 1mm. Functioning masticatory muscles on the right-hand side of the mandible are characterized by loading [-0.6, -0.6, 2.8] $\times 10^6$ N/mm^2 for m. pterygoideus lateralis, [-0.6, 0, 2.8] $\times 10^6$ N/mm^2 for m. masseter and [0, 0.5, 1.5] $\times 10^6$ N/mm^2 for m. pterygoideus medialis. It is evident that on the left-hand side we consider symmetric loading. We assume the model problem in which the heads (condyles) of the TJM and the acetabulae are in mutual contacts, and moreover, for simplicity the acetabulae are assumed to be rigid. The unilateral contact condition on the contact boundary in Fig. 1 is denoted by a yellow colour, for simplicity when we assume that the TMJ is in permanent contact with the skeleton, then it can be replaced by the bilateral contact condition (9).

For the numerical solution the COMSOL Multiphysics with the Structural Mechanics Module were used. The principal stresses are presented in Fig. 2. On

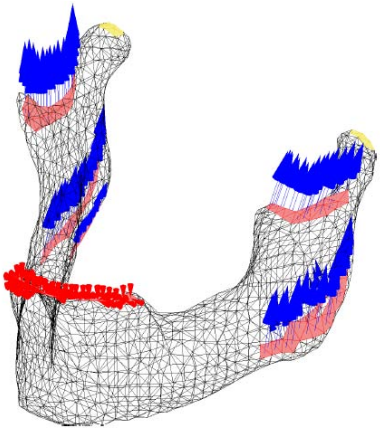


Fig. 1. The finite element mesh and boundary conditions

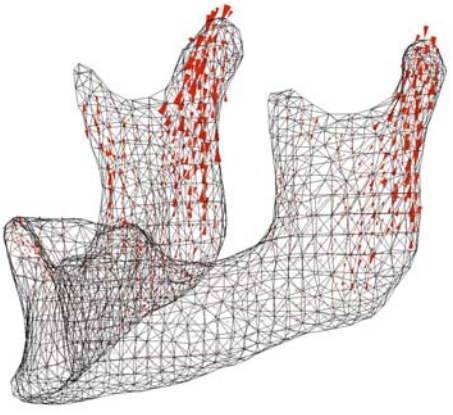


Fig. 2. Distribution of the principal stresses

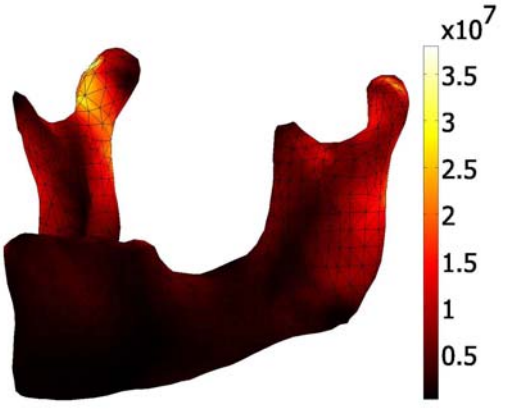


Fig. 3. Distribution of the von Mises stresses

the basis of the TMJ analysis the artificial TMJ replacement can be designed and numerically analysed. In the first step, presented in the previous paper, the healthy TMJ is investigated and analysed. The numerical analysis of the principal and von Mises stresses (see Fig. 3) of the TMJ indicate the highest pressures in the areas of the condyle and the distal part of ramus mandibulae. The comparison with the 2D case (see [5]) and with the observation in dental practice show that the tractions are observed in a good agreement at the muscular processus and at the incisura mandibulae. Numerical results show that the maximal deformations are observed in the area of condyles and the glenoid focca. Numerical data present the values of the maximal pressure in the contact area $\sim 2{,}13 \times 10^7$[Pa] and the magnitudes of principal stresses $\sim 1{,}87 \times 10^7$[Pa].

4 Role of Medical Informatics in Dentist's Decision-Making Temporomandibular Joint Disorders

The unclear etiology of TMD (temporomandibular joint disorders), the same clinical findings resulted from various causes and the proven relation between TMD and psychological factors are the main reasons, why there is still no consensus in classification of TMD [1]. All these mentioned facts make from TMD a very complicated group of diseases for creating a suitable and compact electronic health record system [3]. One of the most commonly used diagnostic schemes intended for the research purposes is the Research Diagnostic Criteria for TMD (RDC/TMD). RDC/TMD standardizes the clinical examination of patients with TMD, improves reproducibility among clinicians and facilitates comparison of results among researchers [1].

TMD are considered to be a subgroup of musculoskeletal disorders [2]. Our application was prepared to produce a user-friendly program, which will unify the whole masticatory system and it's problematic, because all its parts are directly connected. The system was enhanced with the automatic speech recognition module [11] (see Fig. 4). The structure allows a transparent health record on the whole dentition and accomplished examinations of a patient in a concentrated form. The dental information recorded in a common graphical structure accelerates the dentist's decision-making and brings a more complex view on gathered information.

The first and essential step for decision-making in all medical fields, including dentistry, is to structure data and knowledge and to remove or minimize information stored as a free text. If data are structured, then they can be coded by means of international classification systems. Usage of these systems is a crucial step towards interoperability of heterogeneous healthcare records [7]. The formation of classification systems has been motivated mostly by their practical usability in registration, sorting, and statistical processing of medical information. The first interest has been to register incidence of diseases and causes of deaths. Nowadays, there are more than one hundred of various classification systems and thesauri. One of the highly appreciated is SNOMED CT. It is a very complex terminology. Around 50 physicians, nurses, assistants, pharmacists, computer professionals, and other health professionals from the USA and Great Britain participate in its development. Special terminological groups were created for specific terminological fields, such as nursing or pharmacy. SNOMED CT covers 364 400 health terms, 984 000 English descriptions and synonyms, and 1 450 000 semantic relations. Among fields of SNOMED CT belong finding, procedure and intervention, observable entity, body structure, organism, substance, pharmaceutical/biological product, specimen, physical object, physical force, events, environments and geographical locations, social context, context-dependent categories, staging and scales, attribute, and qualifier value. Nowadays we can meet with American, British, Spanish, and German versions of SNOMED CT.

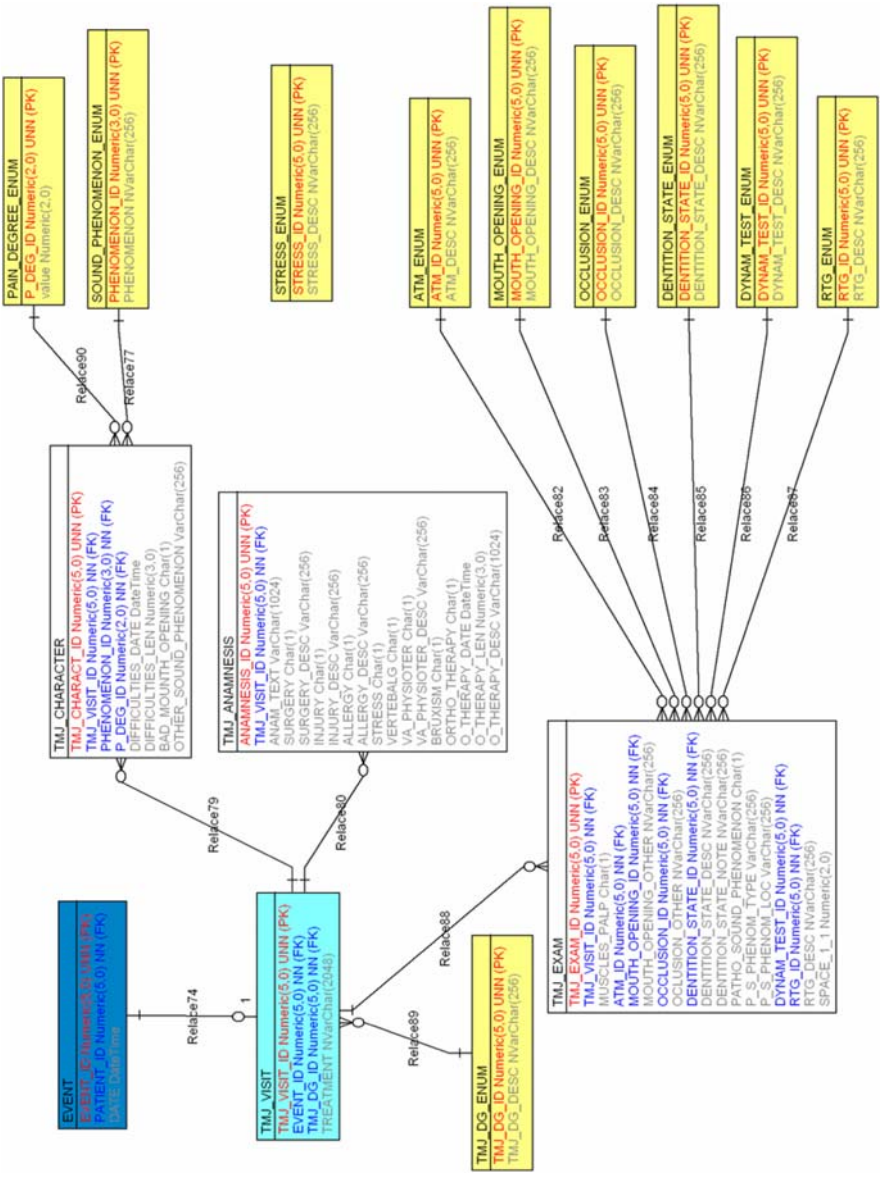


Fig. 4. The automatic speech recognition module

The process of data structuring and coding will lead to sufficient semantic interoperability, which is a basis for shared health care, which will help with efficiency in health care, to financial savings and to reduction of patients' stress. Standardised clinical terminology would bring advantages to physicians, patients, administrators, software developers and payers. Standardised clinical terminology would help providers of shared health care because it would give them more easily accessible and complete pieces of information, which belong to the health care process and it would lead to better care of patients.

5 Concluding Remarks

The analysis of human mandibular motion has been the subject of present-day extensive research. The TMJ is a geometrically complex and extremely mobile joint which motions are characterized by large displacements, rotations and deformations. Mathematical models have been used widely to study muscle tensions, skeletal forces, motions, stresses and deformation of the mandible and the TMJ. All such models are always simplier than the original systems so that they emulate function of the TMJ only approximately. In addition, we need forces to estimate properties of many unknown parts of the TMJ area, unknown muscles as well as inertial data concerning the function of TMJ.

Mathematical and computer modelling of biomechanics of the jaw and the temporomandibular joint have a potential application in many areas of clinical practice, preprosthetic surgery and mandibular reconstruction. Clinical experiences have shown that patients who have had unilateral resection and subsequent reconstruction of the mandible have no pain associated with their reconstructed condyle. Mathematical modelling and mathematical simulation of the reconstruction of the patient jaw and/or patient TMJ may predict the joint loading of the reconstructed condyle. The other applications of mathematical modelling of jaw biomechanics can be useful with force changes and changes of their directions after orthognathic surgery, and moreover, in evaluation of the influence of occlusal splints on TMJ loading as well as in prediction concerning with the tumor cancers.

Previous studies investigated the problem from the kinematic point of view as well as the variation among individuals and they intended to facilitate understanding of the mandibular function and dysfunction. While these previous studies investigate the TMJ kinematically, our approach facillitates to study the stress-strain distribution in all regions and in details in the surroundings of the condyle/disc regions, in the jaw, the mandible, the head, and moreover, it also facillitates to determine the acting contact forces in the condyle/disc areas. Our future main goal of our investigations leads to the development of optimal algorithms for the dynamic contact model problems based on the 3D dynamic primal-dual active set strategy approach in the mathematical case and its application for the dynamic problems in stomatology.

Acknowledgments

The paper was partially supported by the Research Plan MSM4977751301, by the Research project IGA MZCR 9902-4, by the Institutional Research Plan AV0Z10300504 and by the project 1M06014 of the Ministry of Education, Youth and Sports CR.

References

1. Dworkin, S.F., LeResche, L.: Research diagnostic criteria for temporomandibular disorders: review, examinations and specifications criteria. J. Craniomand Disord Facial Oral Pain 6, 301–355 (1992)
2. Goldstein, B.: Temporomandibular disorders: A review of current understanding. Oral Surg Oral Med Oral Pathol Oral Radiol Endod 88, 379–385 (1999)
3. Hippmann, R., Dostálová, T., Zvárová, J., Nagy, M., Seydlová, M., Hanzlíček, P., Kříž, P., Šmídl, L., Trmal, J.: Voice-supported Electronic Health Record for Temporomandibular Joint Disorders. Methods Inf Med. 48(6) (2009)
4. Hlaváček, I., Nedoma, J.: On a Solution of a Generalized Semi-Coercive Contact Problem in Thermo-Elasticity. Math. Comput. Simul. 60, 1–17 (2002)
5. Hliňáková, P., Dostálová, T., Daněk, J., Nedoma, J., Hlaváček, I.: Temporomandibular joint and its two-dimensional and three-dimensional modelling. Math. Comput. Simul (2009) doi:10.1016/j.matcom.2009.08.007
6. Koolstra, J.H., van Eijden, T.M.: The jaw open-close movements predicted by biomechanical modelling. Journal of Biomechanics 30, 943–950 (1997)
7. Nagy, M., Hanzlíček, P., Přečková, P., Kolesa, P., Mišúr, J., Dioszegi, M., Zvárová, J.: Building Semantically Interoperable EHR Systems Using International Nomenclatures and Enterprise Programming Technique. In: eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge, pp. 105–110. IOS Press, Amsterdam (2008)
8. Peck, C.C., Hannam, A.G.: Human jaw and muscle modelling. Arch Oral Biol. 52, 300–304 (2006)
9. Peck, C.C., Murray, G.M., Johnson, C.W.L., Klineberg, I.J.: The varibility of condylar point pathways in open-close jaw movements. J. Prosthet. Dent. 77, 394–404 (1997)
10. Peck, C.C., Langenbach, G.E.J., Hannam, A.G.: Dynamic simulatgion of muscle and articular properties during human wide jaw opening. Archives of Oral Biology 45, 963–982 (2000)
11. Zvárová, J., Dostálová, T., Hanzlíček, P., Teuberová, Z., Nagy, M., Seydlová, M., Eliášová, H., Šimková, H.: Electronic Health Record for Forensic Dentistry. Methods Inf Med. 47(1), 8–13 (2008)

Stability Analysis of an SVLI Epidemic Model

Schehrazad Selmane

LAID3. Faculty of Mathematics
University of Sciences and Technology of Algiers, Algeria
schehrazad.selmane@gmail.com

Abstract. Immunization with the Bacillus Calmette-Guérin (BCG) vaccine is currently used in many parts of the world as a means of preventing tuberculosis even though it remains a highly controversial method of preventing tuberculosis disease. We develop a deterministic mathematical model for the transmission dynamics of tuberculosis to monitor the effect of BCG vaccine, which may wane over time and which is not 100% effective, on tuberculosis epidemiology. The analysis of the presented model has provided conditions to guarantee the eradication of the disease in terms of three major parameters incorporated into the model; the vaccination coverage level, the waning rate and the efficacy of the vaccine.

Keywords: Bacillus Calmette-Guérin (BCG) vaccine; Deterministic model; Equilibria; Reproduction number; Stability; Tuberculosis.

1 Introduction

Tuberculosis (TB) is considered nowadays as the biggest cause of death from preventable and curable infectious diseases with roughly 2 million deaths yearly, besides which approximately one third of the world population is estimated to be infected with Mycobacterium Tuberculosis (MTB), the pathogen of TB. The World Health Organization declared TB a global public health emergency in 1993 and urged governments to improve their national TB programmes; this has resulted in a slight improvement in the TB situation in recent years [7].

Immunization with the Bacillus Calmette-Guérin (BCG), named after the two French investigators responsible for developing the vaccine from an attenuated strain of Mycobacterium bovis, is currently used in many parts of the world as a means of preventing TB. The BCG was first given to humans and used as an anti-tuberculosis vaccine in 1921, and BCG vaccination was encouraged worldwide until the vaccine became, after the eradication of smallpox, the most old and widely used vaccine in the world. However, it remains a highly controversial method of preventing TB disease (TBD) despite more than 88 years of use. Results of randomized controlled trials and case control studies showed the protective efficacy against TB as uncertain and unpredictable, as protective efficacy varied from 0 to 80%. The genetic variability of the subjects vaccinated, the use of different strains of BCG for immunization, the use of different doses of vaccine, and the different schedules of immunization are considered as some factors

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 72–82, 2010.

contributing to variability in the efficacy. It has universally been admitted that BCG vaccination protects small children from severe forms of childhood TB (i.e. miliaire and meningitis), especially in areas with a high risk of infection, where complete coverage of BCG could reduce total TB mortality in children by $4-7\%$. There remain many unanswered questions regarding BCG efficacy in other age groups, but it seems that until better vaccines become available BCG use should be considered for high-risk adults groups, for children who had higher risk of exposure to TB and regions with high prevalence of TB [7].

This work aims to evaluate the effect of a BCG vaccination programme on TB epidemiology, while exploring the impact of three major parameters associated with transmission of TB, namely, vaccination coverage level, efficacy, and waning rate of the BCG vaccine. Such study led to define conditions on these parameters for controlling the spread of TB which may be in aid to the public health policy decisions on the prevention of the disease transmission.

The paper is organized as follows. A deterministic mathematical model to monitor the effect of BCG vaccine on the transmission dynamics of TB, by assuming that the BCG vaccine efficacy is not 100% and may wane with time, is developed in section 2. The stability analysis of the disease free equilibrium, and the existence of endemic equilibria are carried out in section 3. Numerical simulations and brief discussion are reported in section 4.

2 Model Formulation

Typical TB models are usually referred to as $SLIT$ (Susceptible - Latent - Infectious - Treated) models; for a review of mathematical models of TB see for instance [1]. In the aim to evaluate the impact of BCG vaccine on TB incidence; we incorporate into this framework vaccination by splitting the susceptible class into two subclasses, namely, susceptible vaccinated class (V) and susceptible unvaccinated class (S). We will refer to such model a $SVLI$ (Susceptible-Vaccinated-Latent-Infectious) model and we will denote by $S(t)$, $V(t)$, $L(t)$, and $I(t)$ the fraction of susceptible unvaccinated, susceptible vaccinated, latent, and infectious individuals in the population, respectively, at time t. The dynamics of TB and the interaction between these classes and assumptions are assumed as follows :

We assume that the population is homogeneous mixed, and all people are equally likely to be infected by the infectious individuals in a case of adequate contact, and that transmission of the infection occurs with a linear incidence rate. The total population size is assumed to be constant.

We assume that individuals are recruited into the population either by birth or immigration at rate Λ, and a proportion, p, is vaccinated at birth. We assume also that they have never encountered the natural MTB and they can be primary infected only through contact with an infectious individual following the classical mass action incidence. Let β be the transmission coefficient of the disease at primary infection. The unvaccinated individuals become infected at transmission rate β whereas the vaccinated individuals become infected at transmission rate

$\sigma_V \beta$ where σ_V is a factor reducing the risk of infection due to the BCG vaccine; so that $\sigma_V = 0$ means the vaccine is completely effective in preventing infection, while $\sigma_V = 1$ means that the vaccine is completely ineffective. Here we assume that the protection induced by the vaccine is not complete, that is, $0 < \sigma_V < 1$; and we will examine the extreme cases ($\sigma_V = 0$ and $\sigma_V = 1$). Since the BCG vaccine may wane over time, let ω be the rate at which it wanes; that is $1/\omega$ is the duration of loss of immunity acquired by BCG vaccine. A proportion ϕ of susceptibles (respectively, vaccinated) degenerates into active TB whereas the remaining proportion $(1 - \phi)$ degenerates into latent infection. An individual with TB infection progress to active TB at rate α. The recovery rate τ from TB is made up of the rate the recovery with and without treatment, that is, $\tau = \rho + \gamma\theta$ where ρ is recovery rate from active TB without treatment and θ is the probability of successful treatment for detected active TB cases and γ is the detection rate of active TB cases. The natural death rate in each class is assumed to be $\mu > 0$ and infectious have an additional TB induced death rate $m - \mu$. The transfer diagram based on these assumptions is shown in Fig. 1 and lead to the following system of nonlinear ordinary differential equations :

$$\begin{cases} \dot{S} = \Lambda(1-p) - \beta IS + \omega V - \mu S \\ \dot{V} = \Lambda p - \sigma_V \beta IV - (\omega + \mu) V \\ \dot{L} = (S + \sigma_V V)(1-\phi)\beta I + \tau I - (\alpha + \mu) L \\ \dot{I} = (S + \sigma_V V)\phi\beta I + \alpha L - (\tau + m) I \end{cases} \tag{1}$$

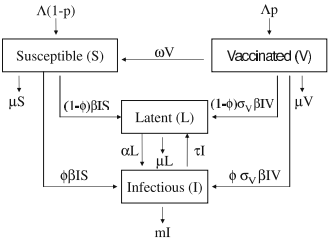


Fig. 1. Flows between the compartments of the model

3 Analysis of the Model

The main goal is the reduction of the number of new cases of TBD to an acceptable level with adequate vaccine coverage level; the eradication of TB can not be achieved nowadays unless a new vaccine is discovered; one of the goals of the global plan to stop TB, 2006-2015. In the terms of a mathematical model, this goal can be achieved when there are no stable positive equilibria, and when the disease free equilibrium (DFE) is stable. In qualitative analysis of the model, the existence of steady states and their stability will be determined and analyzed.

3.1 Steady States

An equilibrium, $E^* = (S^*, V^*, L^*, I^*)$, is a constant solution of system (1). Here, as elsewhere below, the asterisk indicates that the attached quantity is evaluated at equilibrium. Equilibria are obtained by solving the following algebraic system on I^* :

$$\beta I^* S^* - \omega V^* + \mu S^* = \Lambda(1-p) \tag{2}$$
$$\sigma_V \beta I^* V^* + c_1 V^* = \Lambda p \tag{3}$$
$$(S^* + \sigma_V V^*)(1-\phi)\beta I^* + \tau I^* - c_2 L^* = 0 \tag{4}$$
$$(S^* + \sigma_V V^*)\phi\beta I^* + \alpha L^* - c_3 I^* = 0 \tag{5}$$

where $c_1 = \omega + \mu$, $c_2 = \alpha + \mu$, and $c_3 = \tau + m$.
The first three equations (2)-(4) give S^*, V^* and L^* as functions on I^* :

$$V^* = \frac{\Lambda p}{\sigma_V \beta I^* + c_1} \tag{6}$$
$$S^* = \Lambda \frac{(1-p)\sigma_V \beta I^* + (c_1 - p\mu)}{(\beta I^* + \mu)(\sigma_V \beta I^* + c_1)} \tag{7}$$
$$L^* = \frac{\tau\sigma_V \beta^2 I^{*2} + l_1 \beta I^* + l_2}{c_2 (\beta I^* + \mu)(\sigma_V \beta I^* + c_1)} I^* \tag{8}$$

where $l_1 = \Lambda(1-\phi)\sigma_V\beta + \tau(c_1 + \mu\sigma_V)$ and $l_2 = [(c_1 - \mu p) + \mu\sigma_V p]\Lambda(1-\phi)\beta + \tau\mu c_1$. The substitution of S^*, V^* and L^* into the last equation (5) gives either $I^* = 0$, therefore system (1) always has a DFE

$$E_0^* = \left(\frac{c_1 - \mu p}{\mu c_1}\Lambda, \frac{\Lambda p}{c_1}, 0, 0\right), \tag{9}$$

or I^* is a root of the following polynomial :

$$P(X) = \sigma_V \beta^2 X^2 + p_1 \beta X + p_0, \tag{10}$$

where

$$p_1 = \mu\sigma_V (1 - \Re_0) + c_1 \tag{11}$$
$$p_0 = \mu c_1 (1 - \Re) \tag{12}$$

and where $\Re_0$ and $\Re$ are parameters defined by

$$\Re_0 = \frac{\mu\phi + \alpha}{\mu(c_2 c_3 - \alpha\tau)}\Lambda\beta \quad \text{and} \quad \Re = \left(1 - (1-\sigma_V)\frac{\mu}{c_1}p\right)\Re_0 .$$

3.2 Determination of the Effective and Basic Reproduction Numbers

The determination of the reproduction number is a vital first step. We derive from the next generation operator approach [3], the effective reproduction number $\mathfrak{R}$.

Using the same notations as in [2] and letting $X = (S, V)$ (the number non-infected individuals), $Y = (L)$ (the number of infected individuals who do not transmit the disease), $Z = (I)$ (the number of infected individuals capable of transmitting the disease), $E_0^* = (X^*, 0, 0) = (\frac{c_1 - \mu p}{\mu c_1}\Lambda, \frac{\Lambda p}{c_1}, 0, 0)$ the DFE and

$$\widetilde{g}(X^*, Z) = \frac{\left[(c_1 - \mu p + \mu\sigma_V p)\,\Lambda\,(1-\phi)\,\beta + \mu c_1 \tau\right]}{\mu c_1 c_2} I$$

give

$$A = \left(\left[c_2\phi + \alpha\,(1-\phi)\right] \frac{(c_1 - \mu p + \mu p\sigma_V)\,\Lambda\beta}{\mu c_1 c_2} - \frac{\mu c_1\,(c_2 c_3 - \alpha\tau)}{\mu c_1 c_2} \right)$$

Hence

$$M = \left(\left[c_2\phi + \alpha\,(1-\phi)\right] \frac{(c_1 - \mu p + \mu p\sigma_V)\,\Lambda\beta}{\mu c_1 c_2} \right) \texttt{and}\ \ D = \left(\frac{\mu c_1\,(c_2 c_3 - \alpha\tau)}{\mu c_1 c_2} \right)$$

and consequently $\mathfrak{R}$, defined as the spectral radius of the matrix MD^{-1}, is equal to

$$\mathfrak{R} = \left(c_2\phi + \alpha\,(1-\phi)\right)(c_1 - \mu p + \mu p\sigma_V)\,\frac{\Lambda\beta}{\mu c_1\,(c_2 c_3 - \alpha\tau)} \tag{13}$$

which can be re-written as

$$\mathfrak{R} = \left(1 - (1-\sigma_V)\,\frac{\mu}{c_1} p\right)\mathfrak{R}_0 \tag{14}$$

where $\mathfrak{R}_0 = \frac{\mu\phi + \alpha}{\mu(c_2 c_3 - \alpha\tau)}\Lambda\beta$ represents the basic reproduction number, which is defined as the average number of secondary infections produced by an infected individual in a completely susceptible and homogeneous population [3] and corresponding to the vaccination free model $(p = 0)$. When vaccination is present, the obtained threshold quantity $\mathfrak{R}$ (14) is for coverage p, with BCG vaccine assumed to offer a degree of protection $(1 - \sigma_V)$ and to induce immunity that wanes with average of protection $1/\omega$ in a population with average expectation of life $1/\mu$. The expression of $\mathfrak{R}$ shows how much the vaccination reduces the reproduction number and it is clair that $\mathfrak{R} \leq \mathfrak{R}_0$ (since $0 \leq \sigma_V \leq 1$). It shows also that, if the BCG vaccine is considered as a perfect vaccine, that is, $\omega = \sigma_V = 0$, then $\mathfrak{R} = (1-p)\mathfrak{R}_0$, and if the vaccine is considered as completely ineffective, that is, $\sigma_V = 1$, then $\mathfrak{R} = \mathfrak{R}_0$ which confirm the uselessness of vaccination. Finally, considering BCG as a vaccine that offers a complete degree of protection $(\sigma_V = 0)$ with immunity that wanes at the same rate with average death rate $(\omega = \mu)$, or considering it as a vaccine that does not wanes $(\omega = 0)$ but offers only 50% degree of protection $(\sigma_V = 1/2)$ leads to the same threshold quantity, namely, $\mathfrak{R} = (1 - \frac{p}{2})\mathfrak{R}_0$.

3.3 Stability of the Disease Free Equilibrium

The stability of the DFE is achieved through the determination of the sign of the eigenvalues of the jacobian matrix $J_{E_0^*}$ of system (1) evaluated at the DFE

$$J_{E_0^*} = \begin{pmatrix} -\mu & +\omega & 0 & -\beta\frac{c_1-\mu p}{\mu c_1}\Lambda \\ 0 & -c_1 & 0 & -\sigma_V\beta\frac{\Lambda p}{c_1} \\ 0 & 0 & -c_2 & (1-\phi)\,\eta+\tau \\ 0 & 0 & \alpha & \phi\eta - c_3 \end{pmatrix}$$

where $\eta = \left(1-(1-\sigma_V)\,\frac{\mu p}{c_1}\right)\frac{\Lambda\beta}{\mu}$. Two negative eigenvalues $-\mu$ and $-c_1$ are straightforwardly determined; the other two eigenvalues are expressed as the roots of the characteristic equation :

$$\lambda^2 + a_1\lambda + a_2 = 0$$

where

$$a_1 = c_2\left(\frac{(1-\Re)\,\phi c_2 c_3 + \alpha\tau\phi\Re + \alpha\,(1-\phi)\,c_3}{c_2\phi + \alpha\,(1-\phi)}\right) \tag{15}$$

$$a_2 = (c_2c_3 - \alpha\tau)\,(1-\Re)\,. \tag{16}$$

According to the Routh-Hurwitz Criterion, the roots are with negative real parts provided $a_1 > 0$ and $a_2 > 0$. It is clear that inequalities (15) and (16) are fulfilled for $\Re < 1$. Thus, we have established the following lemma.

Lemma 1. *The disease free equilibrium E_0^* is locally asymptotically stable if $\Re < 1$ and unstable $\Re > 1$.*

According to lemma 1, the condition $\Re < 1$ is necessary for disease eradication, however this condition is not sufficient; the local stability of the disease free equilibrium E_0^* does not necessarily imply its global stability.

The level of vaccination coverage that makes $\Re < 1$, called critical vaccination coverage and denoted by p_c, is

$$p_c = \left(1 - \frac{1}{\Re_0}\right)\frac{\omega+\mu}{\mu\,(1-\sigma_V)}$$

which is an increasing function of ω (the rate of loss of immunity). Consequently, improve the vaccine by increasing the duration of loss of immunity $\left(\frac{1}{\omega}\right)$ induced by vaccination reduces the threshold vaccination coverage which is important for the success of public health strategies for controlling TB spread.

3.4 Endemic Equilibrium Points

If the model has a positive equilibrium state and this equilibrium is stable, then all the subpopulation tend to the corresponding equilibrium levels. The disease will persist endemically in this case.

The existence of endemic equilibrium points for system (11) is linked to the existence of real positive roots of the polynomial P (10); the number of infectious individuals must be greater than zero. Hence we determine the conditions under which the polynomial P has real positive root(s). We assume that the protection induced by BCG vaccine is not complete, that is, $0 < \sigma_V < 1$.

• Assume $\Re > 1$, that is $p_0 < 0$. In this case the polynomial P has two real roots of opposite signs. Thus the model has a unique positive endemic equilibrium.

• Now assume that $\Re = 1$, that is $p_0 = 0$. This assumption reduces the polynomial P to $(\sigma_V \beta X + p_1)\beta X$. Since $I^* = 0$ gives the only DFE, therefore P has a unique positive root $\left(I^* = -\frac{p_1}{\sigma_V \beta}\right)$ if $p_1 < 0$ and no positive roots if $p_1 \geq 0$. Thus the model has a unique positive endemic equilibrium if $\Re = 1$ and $\Re_0 > r_0^*$ where

$$r_0^* = 1 + \frac{c_1}{\mu \sigma_V}. \tag{17}$$

• Finally, assume that $\Re < 1$, that is $p_0 > 0$. We have either two positive roots, two negative roots or two complex roots. let Δ be the discriminant of P : $\Delta = \beta^2 p_1^2 - 4\sigma_V \beta^2 p_0$. The polynomial P has two real roots if $\Delta \geq 0$, that is, if $r^* \leq \Re < 1$ where

$$r^* = 1 - \frac{p_1^2}{4\sigma_V \mu c_1}. \tag{18}$$

These roots are positive if moreover $p_1 < 0$, that is, $\Re_0 > r_0^*$. Thus the model has two endemic equilibria if $r^* < \Re < 1$ and $\Re_0 > r_0^*$, and an unique equilibrium of multiplicity 2 if $\Re = r^*$ and $\Re_0 > r_0^*$, and no endemic equilibrium if $\Re < r^*$(the roots are complex) or if $r^* \leq \Re < 1$ and $\Re_0 < r_0^*$ (the roots are negatives).

The following lemma summarises the above results on the existence of endemic equilibria of the model.

Lemma 2. *The model has two positive endemic equilibrium if* $r^* < \Re < 1$ *and* $\Re_0 > r_0^*$.

The model has a unique positive endemic equilibrium if one of the following statements holds :

(i) $\Re > 1$;

(ii) $\Re = 1$ *and* $\Re_0 > r_0^*$

(iii) $\Re < 1$ *and* $\Re = r^*$ *and* $\Re_0 > r_0^*$.

The model has no positive endemic equilibrium if one of the following statements holds :

(i) $\Re = 1$ *and* $\Re_0 \leq r_0^*$

(ii) $\Re < 1$ *and* $\Re < r^*$.

(iii) $\Re < 1$ *and* $r^* \leq \Re < 1$ *and* $\Re_0 < r_0^*$.

Extreme Cases

Let us investigate the existence of endemic equilibria for the model by considering two extreme special cases related to vaccine efficacy and immunity.

– First suppose that the vaccine is completely effective, that is, $\sigma_V = 0$. In this case $I^* = \frac{\mu}{\beta}(\Re - 1)$ and $\Re = \left(1 - \frac{\mu}{c_1}p\right)\Re_0$. Thus, an endemic equilibrium exists if $\Re > 1$ and it is given by

$$\left(\Lambda\frac{(c_1-\mu p)}{\mu c_1 \Re}, \frac{\Lambda p}{c_1}, \frac{\mu c_1 \tau \Re + (c_1-\mu p)\Lambda(1-\phi)\beta}{\beta c_1 c_2}\left(1-\frac{1}{\Re}\right), \frac{\mu}{\beta}(\Re - 1)\right).$$

– Second suppose that the vaccine is useless, that is, $\sigma_V = 1$. In this case $\Re = \Re_0$ and $\Delta = \beta^2(\mu(\Re_0 - 1) + c_1)^2$. Thus P has two real roots $I_1^* = \frac{\mu(\Re_0 - 1)}{\beta}$ and $I_2^* = \frac{-c_1}{\beta}$. Therefore the model has one endemic equilibrium

$$E^* = \left(\Lambda\frac{(1-p)\mu\Re_0 + \omega}{\mu\Re_0(\mu\Re_0 + \omega)}, \frac{\Lambda p}{\mu\Re_0 + \omega}, \frac{\tau\mu\Re_0 + \Lambda(1-\phi)\beta}{c_2\beta}\left(1 - \frac{1}{\Re_0}\right), \frac{\mu}{\beta}(\Re_0 - 1)\right)$$

if $\Re_0 > 1$ and no endemic equilibrium if $\Re_0 < 1$ and the DFE if $\Re_0 = 1$.

4 Numerical Simulation and Discussion

In order to illustrate the obtained theoretical results, we used for the simulations the following biologically feasible parameters where we set a year as an unit of time. Since the model considers human populations, all the model parameters and variables are assumed to be non-negative.

As regards the demographic parameters, the natural mortality was taken to be $\mu = 0.0133yr^{-1}$ corresponding to a life expectancy at birth in Algerian population, which is about $\frac{1}{\mu} = 70\ years$ [4] and we have assumed that the rate at which susceptible individuals are recruited into the population either by birth or immigration balances the deaths and migration, that is, the recruitment rate is $\Lambda = \mu$; a fraction, $p = 80\%$ [5] of recruited individuals is vaccinated. The number of deaths among detected active TB cases in Algeria is around 180 deaths yearly [5], so we can assume without loss of generality that $m = \mu$.

As regards parameters modelling the progression to active TB and following estimates of Vynnycky and Fine [6], we set $\phi = 11\%$ and $\alpha = 0.03\%$ per year. Besides which BCG vaccination has only a small role in reducing the population incidence and transmission of TB, there is widespread general agreement that the efficacy of BCG at its best is about 80 % and of $15 - 20$ years duration. For the simulations for the rate of loss of immunity induced by BCG vaccine and the efficacy of the vaccine, we used several values. As for β it was chosen so that $\Re > 1$; the disease being endemic in Algeria. The proportion of successful treatment for detected active TB cases is approximately 90%, we take this value for θ and the detection rate of active TB cases is approximately 70%, we take this value for γ [5]. For the recovery rate from active TB without treatment we chose $\rho = 0.25$ per year [6]. With these choices, we obtain $\tau \simeq 0.88$

Fig. 2 (resp. Fig. 3) shows how the proportion of infectious (resp. latent TB) individuals changes over time where the initial values were fixed from Algerian data : population size $N = 34000000$; $I_0 = 21077/N$; $L_0 = I_0/\phi$; $S_0 = (1 - I_0 - L_0)(1 - p)$; $V_0 = (1 - I_0 - L_0)p$ [5] and this for fixed value of $\sigma_V = 0.2$

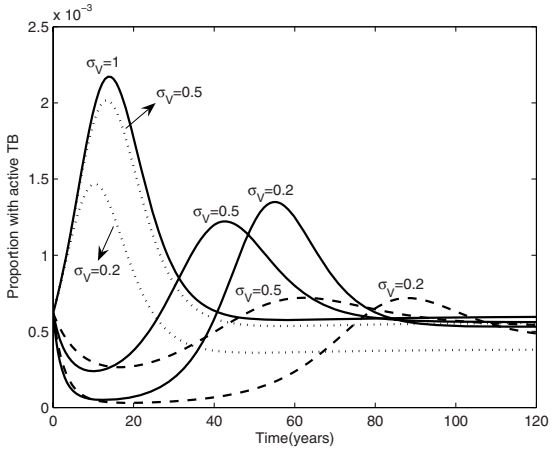


Fig. 2. Simulation curves show how the population of TB infectious individuals evolves over time. Solid lines tally to $\omega = 1/15$, dashed lines tally to $\omega = \mu$, and dotted lines tally to $\omega = 0$.

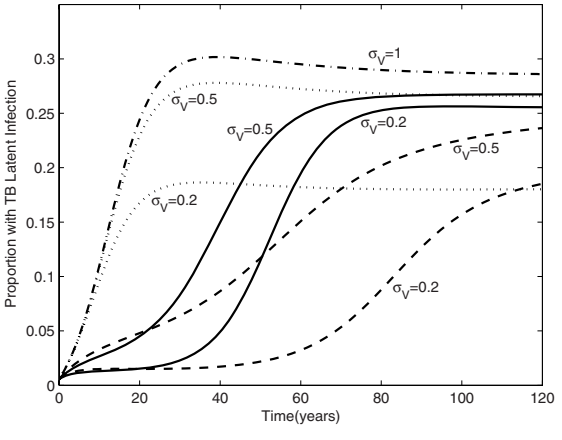


Fig. 3. Simulation curves show how the proportion of Latent TB individuals evolves over time. Solid lines tally to $\omega = 1/15$, dashed lines tally to $\omega = \mu$, and dotted lines tally to $\omega = 0$ and dash-dotted line tally to $\omega = 0,\ 1/15,\ \mu$.

(resp. 0.5, 1) and $\omega = 0$ (resp. $1/15$, μ), and β was fixed so that $\mathfrak{R} = 1.4$. These simulations demonstrate an initial drop in the number of detected infectious cases for $\omega = 1/15$ and $\omega = \mu$, which is followed by a gradual increase, and the effect on the proportion of latent TB. It appears that the introduction of treatment of all detected infectious individuals led to the drop in this class, and the rise in the number of active TB cases maybe attributed to a lack of efficient system of detection at early stages of infection.

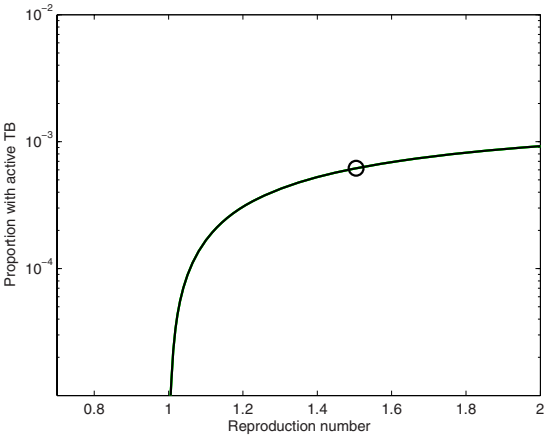


Fig. 4. Proportion of individuals with active TB at equilibrium as a function of the reproduction number. The circle ∘ corresponds to the proportion of TB infectious individuals in Algeria for the year 2008.

Fig. 4 describes how the proportion of infectious individuals evolve at equilibrium as a function of the reproduction number $\mathcal{R}$.

Without vaccination the disease will persist, but if everyone were vaccinated, the disease normally die out but TB remains an established disease. The model shows that bringing the effective reproduction number beneath 1 is not sufficient to eradicate the disease, two new threshold must be satisfy and the eradication depends on vaccination coverage as well as on vaccine efficacy and vaccine induced immunity.

Acknowledgments. I am grateful to Chris Bauch and Gabriela Gomes for their supports.

References

1. Castillo-Chavez, C.: Dynamical models of Tuberculosis and their applications. Mathematical biosciences and engineering 1, 361–404 (2004)
2. Castillo-Chavez, C., Feng, Z., Huang, W.: On the computation Ro and its role on global stability. In: Castillo-Chavez, C., Blower, S., van den Driesschie, Kirschner, D., Yakubu, A.A. (eds.) Mathematical Approaches for Emerging and Reemerging Infectious Diseases: An Introduction, IMA Volumes in Mathematics and its Applications, vol. 125, pp. 229–250. Springer, Heidelberg (2002)
3. Diekmann, O., Heesterbeek, J.A.P., Metz, J.A.J.: On the definition and the computation of the basic reproductive ratio R_0 in models of infectious diseases in heterogeneous populations. J. Math. Biol. 28(4), 365–382 (1990)
4. National Office of Statistics, http://www.ons.dz

5. INSP: Relevé Epidémiologique Mensuel (REM), 2000 à 2006, http://www.insp.dz
6. Vynnycky, E., Fine, P.E.M.: The natural history of tuberculosis: the implications of age-dependent risks of disease and the role of. Epidemiol. Infect. 119, 183–201 (1997)
7. World Health Organization (WHO), Global tuberculosis control: surveillance, planning, financing: WHO report 2008, WHO/HTM/TB/2008.393 (2008)

A New Expert System for Diabetes Disease Diagnosis Using Modified Spline Smooth Support Vector Machine

Santi Wulan Purnami[1,2], Jasni Mohamad Zain[1], and Abdullah Embong[1]

[1] Faculty of Computer System and Software Engineering, University Malaysia Pahang, Lebuh Raya Tun Abdul Razak 26300, Kuantan Pahang, Malaysia
[2] Department of Statistics, Institute of Technology Sepuluh Nopember (ITS) Surabaya Keputih, Sukolilo, Surabaya 60111, Indonesia

Abstract. In recent years, the uses of intelligent methods in biomedical studies are growing gradually. In this paper, a novel method for diabetes disease diagnosis using modified spline smooth support vector machine (MS-SSVM) is presented. To obtain optimal accuracy results, we used Uniform Design method for selection parameter. The performance of the method is evaluated using 10-fold cross validation accuracy, confusion matrix, sensitivity and specificity. The comparison with previous spline SSVM in diabetes disease diagnosis also was given. The obtained classification accuracy using 10-fold cross validation is 96.58%. The results of this study showed that the modified spline SSVM was effective to detect diabetes disease diagnosis and this is very promising result compared to the previously reported results.

Keywords*:* classification, diabetes disease diagnosis, smooth support vector machine, modified spline function.

1 Introduction

There is considerable increase in the number of diabetes disease cases in recent years. During the last 20 years the total number of people with diabetes worldwide has risen from 30 million to 230 million, according to the International Diabetes Federation [1]. And there are 6 million new diabetes sufferers in the world each year. Now, diabetes is the fourth biggest cause of death worldwide. Diabetes causes more cases of blindness and visual impairments in adults than any other illness in develop word. One million amputations each year are caused by diabetes [1].

There are many factors to analyze to diagnose the diabetes of a patient, and this makes the physician's job difficult. To help the experts and helping possible errors that can be done since of fatigued or inexperienced expert to be minimized. In the last few decades, computational tools have been designed to improve the experiences and abilities of physicians for making decisions about their patients. In this study, we propose a new method to efficiently diagnose the diabetes disease. The proposed method uses modified spline SSVM (MS-SSVM). To achieve high accuracy results, we used uniform design method for selection parameter. The dataset that is used in this study is Pima Indian Diabetes that was obtained from UCI machine learning repository [9]. The obtained classification accuracy is 96.58% using 10-fold cross validation.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 83–92, 2010.

The rest of the paper is organized as follows: In section 2, we describe the proposed methods. Firstly the modified spline smooth support vector machine is presented, and then we describe the outline of uniform design to select the optimal parameter. In section 3, the experiment and results are presented. Finally, discussion and conclusions is given in section 4.

2 The Proposed Method

2.1 Overview

The proposed method consists of two main parts: modified spline SSVM for classification and uniform design method for selection parameters. First, we explain the outline SSVM, and then the modified spline SSVM is described.

Smooth Support Vector Machine (SSVM). SSVM is proposed by Lee and Mangasarian [7]. In this session, we describe the outline of reformulation standard SVM [14] to SSVM. We begin with the linear case which can be converted to an unconstrained optimization problem. We consider the problem of classifying *m* points in the *n*-dimensional real space R^n, represented by the *m x n* matrix *A*, according to membership of each point A_i in the classes 1 or -1 as specified by a given *m x m* diagonal matrix *D* with ones or minus ones along its diagonal. For this problem the standard SVM is given by the following quadratic program:

$$\min_{(w,\gamma,y)\in R^{n+1+m}} \nu e'y + \frac{1}{2}w'w$$

$$\text{s.t. } D(Aw - e\gamma) + y \geq e$$

$$y \geq 0 \tag{1}$$

Where, ν is a positive weight, *y* is slack variable and *e* is column vector of one of arbitrary dimension. Here *w* is the normal to the bounding planes:

$$x'w - \gamma = +1$$
$$x'w - \gamma = -1 \tag{2}$$

γ determines their location relative to the origin. The linear separating surface is the plane:

$$x'w = \gamma \tag{3}$$

If the classes are linearly inseparable, the bounding plane as follows:

$$x'w - \gamma + y_i \geq +1, \text{ for } x' = A_i \text{ and } \quad D_{ii} = +1,$$
$$x'w - \gamma - y_i \leq -1, \text{ for } x' = A_i \text{ and } \quad D_{ii} = -1, \tag{4}$$

These constraints (4) can be written as a single matrix equation as follows:

$$D(Aw-e\gamma)+y\geq e \tag{5}$$

In the SSVM approach, the modified SVM problem is yielded as follows:

$$\min_{(w,\gamma,y)\in R^{n+1+m}} \frac{v}{2}y'y+\frac{1}{2}(w'w+\gamma^2)$$

$$\text{s.t. } D(Aw-e\gamma)+y\geq e$$

$$y\geq e \tag{6}$$

The constraint in equation (6), can be written by

$$y=(e-D(Aw-e\gamma))_+ \tag{7}$$

Thus, we can replace y in constraint (6) by (7) and convert the SVM problem (6) into an equivalent SVM which is an unconstrained optimization problem as follows:

$$\min_{(w,\gamma)} \frac{v}{2}\left\|(e-D(Aw-e\gamma))_+\right\|_2^2+\frac{1}{2}(w'w+\gamma^2) \tag{8}$$

The plus function $(x)_+$, is defined as

$$(x)_+=\max\{0,x_i\},\ i=1,2,3\ldots n \tag{9}$$

The objective function in (8) is undifferentiable and unsmooth. Therefore, it cannot be solved using conventional optimization method, because it always requires that the objective function's gradient and Hessian matrix. Lee and Mangasarian [7] apply the smoothing techniques and replace x_+ by the integral of the sigmoid function:

$$p(x,\alpha)=x+\frac{1}{\alpha}\log(1+\varepsilon^{-\alpha x}),\ \alpha>0 \tag{10}$$

This p function with a smoothing parameter α is used here to replace the plus function of (8) to obtain a smooth support vector machine (SSVM):

$$\min_{(w,\gamma)\in R^{n+1}} \frac{v}{2}\left\|p(e-D(Aw-e\gamma),\alpha)\right\|_2^2+\frac{1}{2}(w'w+\gamma^2) \tag{11}$$

For nonlinear un-separable problem requires choosing kernel function K to reflect the input space into another space. This model was derived from Generalized Support Vector Machines [8]. So the problem (6) can be approximated as following:

$$\min_{(u,\gamma,y)} \frac{v}{2}y'y+\frac{1}{2}(u'u+\gamma^2)$$

$$\text{s.t. } D(K(A,A')Du-e\gamma)+y\geq e$$

$$y\geq 0 \tag{12}$$

Same as previous, it is obtained the SSVM for inseparable problem:

$$\min_{(u,\gamma)} \frac{v}{2}\left\|p(e-D(K(A,A')Du-e\gamma),\alpha)\right\|_2^2+\frac{1}{2}(u'u+\gamma^2) \tag{13}$$

Where $K(A,A')$ is a kernel map from $R^{mxn} xR^{nxm}$ *to* R^{mxm}. We use Radial Basis Function kernel as follows:

$$e^{-\mu\left\|A_i - A_j\right\|_2^2}, \quad i,j = 1,2,3....m \tag{14}$$

Modified Spline Smooth Support vector machine (MS-SSVM). SSVM which has been proposed by Lee, et al [7] is very important and significant result to SVM because many algorithms can be used to solve it. In SSVM, the smooth function in objective function (13) is the integral of sigmoid function (10) to approximate the plus function. In this paper, we propose a new smooth function which called modified spline function instead the integral of sigmoid function.

The modified spline function is modification of the three order spline function introduced by Yuan, et al [13]. We recall the three order spline function as follows:

$$t(x,k) = \begin{cases} 0, & if\ x < -\frac{1}{k} \\ \frac{k^2}{6}x^3 + \frac{k}{2}x^2 + \frac{1}{2}x + \frac{1}{6k}, & if\ -\frac{1}{k} \le x < 0 \\ -\frac{k^2}{6}x^3 + \frac{k}{2}x^2 + \frac{1}{2}x + \frac{1}{6k}, & if\ 0 \le x \le \frac{1}{k} \\ x, & if\ \frac{1}{k} < x \end{cases} \tag{15}$$

And we proposed the modified spline function as follows:

$$m(x,k) = \begin{cases} 0, & if \quad x < \dfrac{-1}{k} \\ \dfrac{k^2x^3}{6} + \dfrac{kx^2}{2} + \dfrac{1}{2}x + \dfrac{1}{6k}, & if \quad \dfrac{-1}{k} \le x < \dfrac{-2}{5k} \\ \dfrac{25}{18}k^2x^3 + \dfrac{5}{4}kx^2 + \dfrac{4}{9}x + \dfrac{1}{10k}, & if \quad \dfrac{-2}{5k} \le x < \dfrac{2}{5k} \\ -\dfrac{k^2x^3}{6} + \dfrac{kx^2}{2} + \dfrac{1}{2}x + \dfrac{1}{6k}, & if \quad \dfrac{2}{5k} \le x < \dfrac{1}{k} \\ x, & if \quad x \ge \dfrac{1}{k} \end{cases} \tag{16}$$

In order to show the difference between the integral of sigmoid function $p(x,k)$, three order spline function $t(x,k)$ and modified spline function $m(x,k)$ more clearly, we present the following comparison figure (fig. 1). The smooth parameter is set at $k = 10$. As can be seen from figure 1, our proposed function is closer to the plus function than sigmoid function $p(x,k)$ and three order spline function $t(x,k)$, which indicates the superiority of our proposed smooth function.

This function will be used to construct a new smooth support vector machine. If we replace the plus function in problem (13) by modified spline function (16), a new SSVM model is obtained as following:

$$\frac{v}{2}\left\|m\left(e - D\left(K(A,A')Du - e\gamma\right),\alpha\right)\right\|_2^2 + \frac{1}{2}\left(u'u + \gamma^2\right) \tag{17}$$

It is called the Modified Spline Smooth Support Vector Machines (MS-SSVM). We use Newton Armijo algorithm to solve the MS-SSVM

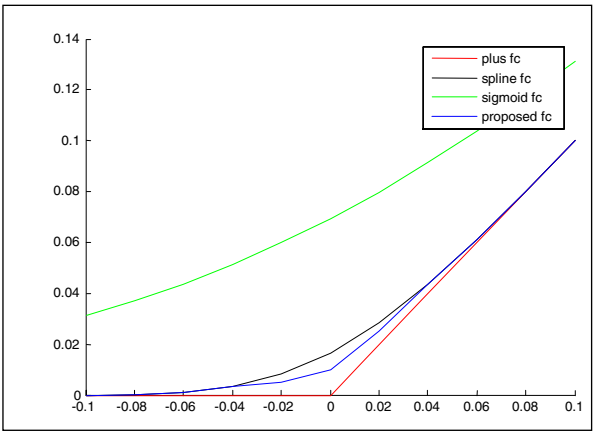


Fig. 1. Comparison figure of the integral of sigmoid function $p(x,k)$, three order spline function $t(x,k)$ and modified spline function $m(x,k)$

2.2 Parameter Selection Using Uniform Design

There are two parameters which we must automatically tune in this parameter selection: the MS-SVM regularization parameter ν and kernel parameter μ. In this work, we use Radial Basis Function (RBF) kernel since it has a few numbers of parameters and has less numerical difficulties [3]. If the kernel function has been chosen, the next problem is choosing a good parameter setting for better generalization ability. In parameter selection problems, the most common estimate methods to independently evaluate the performance of methods are *k*-fold cross validation (*k*-CV) and leave one out (LOO) [3]. We used 10-fold CV for this experiment. Except the estimation method, the mechanism of searching for parameter sets that make SVM resulting model perform well is important, too. The most common and reliable approach for model selection is exhaustive grid search method [3]. The other method, a new approach has been proposed by Huang, *et al* [2] which is known *Uniform Design* (UD) method. The steps to implement the uniform design in MS-SSVM parameter selection problem as follows:

1. Choose a parameter search domain; determine a suitable number of levels for each parameter. In this work, levels of parameter ν = [2^{-5}, 2^{15}] and levels of parameter μ = [2^{-5}, 2^{3}].
2. Choose a suitable UD table to accommodate the number of parameters and levels. This can be easily done by visiting the UD-web.
   http://www.math.hkbu.edu.hk/UniformDesign.
3. From the UD table, randomly determine the run order of experiments and conduct the performance evaluation of each parameter combination in the UD.
4. Fit the MS-SSVM model.
5. Find the best combination of the parameter values that maximizes the performance measure.

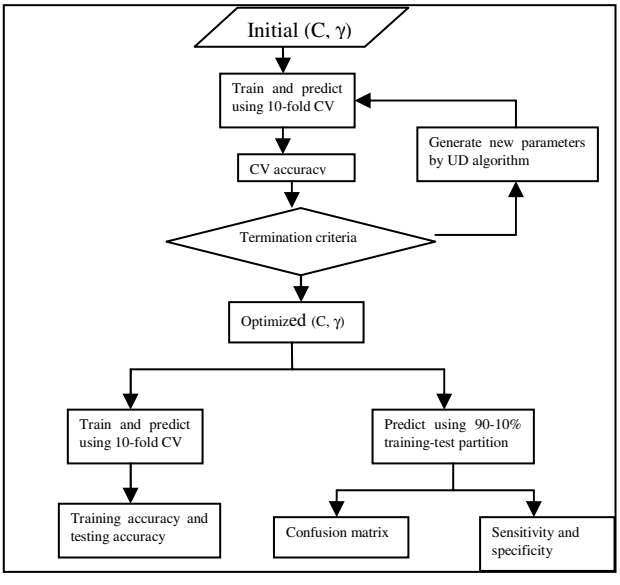


Fig. 2. The modified spline SSVM strategy using Uniform Design

More detail, the MS-SSVM based strategy using UD design to optimize model parameters can be described in fig.2.

3 The Experiment and Results

3.1 Data Description

The medical dataset which used in our works is Pima Indian Dataset [9]. The dataset contains 768 samples and two classes. All patients in this database are Pima-Indian women at least 21 years old and living near Phoenix, Arizona, USA. The class distribution is:

- Class 1: normal (500)
- Class 2: Pima Indian diabetes (268)

All samples have eight features. These features are:

1. Number of time pregnant.
2. Plasma glucose concentration a 2 h in oral glucose tolerance test.
3. Diastolic blood pressure (mm Hg).
4. Triceps skin fold thickness (mm).
5. 2-h serum insulin (μ U/ml).
6. Body mass index (weight in kg/(height in m)^2).
7. Diabetes pedigree function.
8. Age (years).

3.2 Previous Studies on Diabetes Disease

There has been a lot of research on medical diagnosis of diabetes disease in literature, and most of them reported not too high classification accuracies. In Polat et al. [11], a cascade learning system based on Generalized Discriminant Analysis (GDA) and Least Square Support Vector Machine (LS-SVM) was used. They have reported 78.21% classification accuracy using LS-SVM with 10-fold cross validation (10 x CV). They have also reported 79.16% classification accuracy using GDA-LS-SVM. Polat and Gunes [10] have reported 89.47% using Principal Component Analysis (PCA) and Adaptive Neuro-Fuzzy Inference System (ANFIS). The accuracy obtained by Kayaer and Yildirim [5] using General Regression Neural Network (GRNN) was 80.21%, while using Multilayer Neural Network (MLNN) with LM algorithm was 77.08%. Temurtas, H et al [12] applied MLNN with LM and Probabilistic Neural Network (PNN) for diagnosing Pima Indian diabetes. They have reported 79.62% classification accuracy using MLNN with 10-fold CV and 82.37% accuracy with conventional (one training and one test) validation method. They have also reported 78.05% classification accuracy using PNN 10-fold CV and 78.13% accuracy using conventional validation method. There have been several other studies reported with accuracy between 59.5% and 84.2%. The detail accuracy of these studies can be seen in Kahramanli, H and Allahverdi, N [4]. The summary of previous researches as mentioned above can be seen in following Table 1.

Table 1. Classification accuracies obtained with our method and other classifiers

Author (year)	Method	Classification accuracy (%)
Kayaer and Yildrim (2003)	GRNN	80.21
	MLNN with LM	77.08
Polat and Gunes (2007)	PCA-ANFIS	89.47 (not reproducible)
Polat *et al*. (2008)	LS-SVM	78.21
	GDA-LS-SVM	79.16
Temurtas, H. *et al*. (2009)	MLNN with LM (10×FC)	79.62
	PNN (10×FC)	78.05
	MLNN with LM (conventional valid)	82.37
	PNN (conventional valid)	78.13
Kahramanli, H and Allahverdi, N (2008)	Various method	Between 59.5 and 84.2
Our study (2009)	Modified spline SSVM	**96.58**

3.3 Performance Evaluation

We present the performance evaluation methods which used to evaluate the MS-SSVM method. There are four methods for performance evaluation of medical diagnosis. These methods are 10-fold cross validation accuracy, confusion matrix, classification accuracy, analysis of sensitivity and specificity. We explain these methods in the following sections.

Ten fold cross validation (10-CV). To guarantee that the present results are valid and can be generalized for making predictions regarding new data, the data set is randomly partitioned into training and testing sets via 10-fold CV. In 10-fold CV, the data set is divided into 10 subsets, and the holdout method is repeated 10 times. Each time, one of the 10 subsets is used as the test set and the other 9 subsets are put together to form a training set. The 10- fold cross validation included training accuracy and testing accuracy. Training accuracy/testing accuracy are average of training accuracy/testing accuracy in 10 trials.

Confusion matrix. A confusion matrix [6] contains information about actual and predicted classifications done by a classification system. Table 2 shows the confusion matrix for a two class classifier. The entries of our confusion matrix are explained:

- *TN* is the number of *correct* predictions that an instance is *negative*
- *FP* is the number of *incorrect* predictions that an instance is *positive*
- *FN* is the number of *incorrect* predictions that an instance is *negative*
- *TP* is the number of *correct* predictions that an instance is *positive*

Table 2. Representation of confusion matrix

Actual	predicted	
	Negative	Positive
Negative	True Negative (TN)	False Positive (FP)
Positive	False Negative (FN)	True Positive (TP)

Classification accuracy, sensitivity, specificity value can be defined by using the elements of the confusion matrix.

Classification Accuracy. In this study, the classification accuracies for the datasets are measured based on Table 2:

$$Classification\ accuracy(\%) = \frac{TN + TP}{TP + FP + FN + TN} \tag{18}$$

Sensitivity and Specificity. For sensitivity and specificity analysis, we use the following expressions:

$$sensitivity\ (\%) = \frac{TP}{TP + TN} \tag{19}$$

$$specificity\ (\%) = \frac{TN}{FP + TN} \tag{20}$$

The sensitivity is classification accuracy rates for positive case and the specificity is classification accuracy rates for negative case.

3.4 Results

To evaluate the effectiveness of our method, we conducted experiments on the Pima Indian Diabetes dataset mentioned above. We compare our result with previous

studies reported. Table 1 gives the classification accuracies of our method and other classifiers. It can be seen that, our method using 10-fold cross validation obtains the highest classification accuracy so far.

In this study, we also compare our method with previous spline SSVM. As can be seen in Table 3, the 10-fold accuracy (training accuracy and testing accuracy) for spline SSVM and modified spline SSVM are same. Using Uniform design method, the optimal parameters are $\nu = 316.2278$ and $\mu = 0.1403$. For next analysis, we use these parameters to compute confusion matrix, classification accuracy, sensitivity and specificity.

Table 3. 10-fold cross validation accuracy

10-fold CV	Spline SSVM	Modified spline SSVM
Training accuracy (%)	96.62	96.62
Testing accuracy (%)	96.58	96.58

In Pima Indian diabetes study, there were two diagnose classes: normal (healthy) and a patient who is subject to possible diabetes disease. Classification results of the system were displayed by using a confusion matrix in Table 4. From Table 4, it can be seen that none number of incorrect predictions that an instance is normal. Whereas, the number of incorrect of predictions that an instance are 5 and 4 for the spline SSVM and the modified spline SSVM, respectively.

Table 4. Confusion matrix using spline SSVM and modified spline SSVM for 90-10% training-test partition

actual	predicted		method
	Normal	disease	
normal	46	0	Spline SSVM
disease	5	26	
normal	46	0	Modified spline
disease	4	27	SSVM

The obtained classification accuracies, sensitivity and specificity analysis value by spline and modified spline SSVM are shown in Table 5. As can be seen in Table 5 classification accuracy rates, classification accuracy rates for positive case and classification accuracy rates for negative case of the modified spline SSVM are 94.81%, 100% and 92%, respectively. This is slightly better performance than previous spline SSVM.

Table 5. Obtained classification accuracy, sensitivity and specificity for 90-10% training-test partition

measures	Spline SSVM	Modified spline SSVM
Classification accuracy (%)	93.51	94.81
Sensitivity (%)	100	100
Specificity (%)	90.19	92.00

4 Discussion and Conclusions

In this study, a new method for diabetes disease diagnosis using modified spline SSVM is presented. In order to achieve high classification accuracy, the uniform design approach was used to select the optimal modified spline SSVM parameters. The comparisons of classification accuracies of previous studies and previous spline SSVM for Pima Indian diabetes datasets are shown in Table 3 and Table 1, respectively. The proposed method achieved the highest accuracy rate when comparing the related previous studies and slightly better accuracy rate than previous spline SSVM.

From the results above can be concluded that the modified spline SSVM is effective to detect diabetes disease diagnosis and this is very promising result compared to the previously reported results.

References

1. Medical News Today, http://www.medicalnewstoday.com/articles/44967.php
2. Huang, C.M., Lee, Y.J., Lin, D.K.J., Huang, S.Y.: Model Selection for Support Vector Machines via Uniform Design. A Special issue on Machine Learning and Robust Data Mining of Computational Statistics and Data Analysis 52, 335–346 (2007)
3. Hsu, C.W., Chang, C.C., Lin, C.J.: Practical Guide To Support Vector Classification. Department of Computer Science and Information Engineering National Taiwan University (2003), http://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf
4. Kahramanli, H., Allahverdi, N.: Design of A Hybrid System for The Diabetes and Heart Diseases. Expert Systems with Applications 35, 82–89 (2008)
5. Kayaer, K., Yildirim, T.: Medical Diagnosis on Pima Indian Diabetes using General Regression Neural Networks. In: Proceedings of the International Conference on Artificial Neural Networks and Neural Information Processing, June 26-29, pp. 181–184. Springer, Istanbul (2003)
6. Kohavi, R., Provost, F.: Glossary of terms. Editorial for the Special Issue on Applications of Machine Learning and the Knowledge Discovery Process 30, 2–3 (1998)
7. Lee, Y.J., Mangasarian, O.L.: A Smooth Support Vector Machine. J. Comput. Optimiz. Appli. 20, 5–22 (2001)
8. Mangasarian, O.L.: Generalized Support Vector Machines. In: Smola, A., Bartlett, P., Scholkopf, B., Schurrmans, D. (eds.) Advances in large Margin Classifiers, pp. 35–146. MIT Press, Cambridge (2000)
9. Newman, D.J., Hettich, S., Blake, C.L.S., Merz, C.J.: UCI repository of machine learning database, Irvine, CA: University of California, Dept. of Information and Computer Science (1998), http://www.ics.uci.edu/~mlearn/~MLRepository.html
10. Polat, K., Gunes, S.: An Expert System Approach Based on Principal Component Analysis and Adaptive Neuro-Fuzzy Inference System to Diagnosis of Diabetes Disease. Digital Signal Processing 17, 702–710 (2007)
11. Polat, K., Gunes, S., Aslan, A.: Cascade Learning System for Classification of Diabetes Disease: Generalized Discriminant Analysis and Least Square Support Vector Machine. Expert System with Applications 34, 214–222 (2008)
12. Temurtas, H., et al.: A Comparative Study on Diabetes Disease Using Neural Networks. Expert System with Applications 36, 8610–8615 (2009)
13. Yuan, Y., Fan, W., Pu, D.: Spline Function Smooth Support Vector Machine for Classification. J. Ind. Manage. Optimiz. 3, 529–542 (2007)
14. Vapnik, V.: The Nature of Statistical Learning Theory, 2nd edn. Springer, New York (1995)

Information Privacy in Smart Office Environments: A Cross-Cultural Study Analyzing the Willingness of Users to Share Context Information

Carsten Röcker

Human Technology Centre (Humtec), RWTH Aachen University
Theaterplatz 14, 52056 Aachen, Germany
roecker@humtec.rwth-aachen.de

Abstract. This paper presents a cross-cultural study analyzing the willingness of users to share context information in work environments. The focus of the study is on three aspects: the general willingness to provide different types of context information, the acceptance of manual and automated data capturing mechanisms and the identification of personal and cultural differences among users. The results of the study show that potential users are rather reluctant to provide context information, especially if the data is automatically captured by the system, and that the willingness to provide context information differs significantly between user groups with different cultural backgrounds and different degrees of computer knowledge.

Keywords: Context-Awareness, Privacy, Ubiquitous Computing, Pervasive Computing, Ambient Intelligence, Evaluation, Technology Acceptance.

1 Introduction

Over the last few years, companies started to show an increased interest in deploying Ambient Intelligence technologies to realize the benefits, offered by location- and context-aware systems (see, e.g., [32], [33] or [33]). In general, such systems enable office workers to communicate, collaborate and work in new and more efficient ways. The theoretical advantages range from increased work productivity through time-saving operations to higher work satisfaction through attentive and reactive environments. Especially the advances in the area of interface technology are expected to lead to considerable benefits. Today, office workers usually work with single user devices, which require manual user input via standardized interfaces. With the emergence of context-aware systems those explicit and static interaction paradigms will be enhanced through new input and output concepts. Sensor-enhanced environments will enable implicit interaction mechanisms, which are unknown in existing work environments with traditional computational devices. By automating routine task and thereby releasing office workers from vacuous work activities, context-aware office environments also bear the potential to increase overall job satisfaction. But in order for these benefits to occur, it is necessary, that the technology is used and also incorporated into the daily routines of employees [28]. Empirical evidence shows, that one of the main reasons for low returns of investment of new technologies is the poor

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 93–106, 2010.

usage of the installed applications (see, e.g., [8], [9] or [15]). In the majority of cases, the potential of the implemented applications is not fully realized, due to the reservations of users to fully incorporate the systems into their daily working routines [6].

2 Research Goal

For their operation, context-aware systems rely on appropriate and sufficient information from users. This information may include their location, identity, and usage patterns of systems or services, and it might be collected by explicit and implicit means. Besides general design and usability problems, most problems encountered in existing applications are associated with a new quality of data collection, that goes far beyond the capabilities of existing computational systems. The two most important differences in this context are the always-on nature of the devices and the invisibility of the technology. With traditional computers, the duration of data collection and potential surveillance is clearly limited to the time, a person uses the system. But in context-aware environments this clear distinction between 'online' and 'offline' might not longer be possible. At the same time the integration of computers into everyday objects is likely to lead to the disappearance of sensory borders, and thereby could make common principles of privacy protection useless [23].

In order to be able to design trusted systems, it is important to be aware of the concerns and perceived threats of potential end users regarding the collection of context information. Therefore, the goal of this paper is to identify the willingness of users to provide different types of context information as well as the preferred level of control over the employed capturing mechanisms, which are necessary to provide context-adapted services. In addition, the paper aims to explore the existence of inter-personal and inter-cultural differences among different groups of users. Technology diffusion studies conducted in the past suggest that there are significant inter-personal differences in the adoption process of new technologies (see, e.g., [2] for a comprehensive study on how individual differences affect usage). Especially when designing context-aware work spaces, it is essential to support a very heterogeneous group of users, as the developed devices will be available throughout a shared environment and are used by multiple users. While there are various individual difference that are likely to play a role in the adoption process, in particular cultural differences are becoming increasingly important, as more and more people are working in multi-national corporations or are collaborating in distributed teams with colleagues all over the world. Therefore, this paper will have a special focus on the identification of cultural differences, which influence the willingness of users to provide context information as well as the preferred level of control over the associated data capturing mechanisms.

3 Conceptual Approach

As explained above, it is expected that the users' willingness to provide context information depends on (at least) three aspects: the type of information that is being collected, the way the data capturing mechanisms are implemented, and the personal and cultural background of the user. Prior to the evaluation, all three factors were carefully examined. The insights gained in this process are briefly illustrated in the next sections.

3.1 Identification of Relevant Information Types

In a first step, existing application scenarios and prototype applications were analyzed in order to identify representative functionalities of state-of-the-art systems (see [31] for more details on the survey). This information was then used to distil the overall information requirements of context-aware office applications based on generic information types. The analysis revealed, that several types of information are necessary in order to provide state-of-the-art functionalities. These types include data about the identity of users, their location and activity, availability information, biometric information, personal preferences as well as information about planned activities in the future (see Tab. 1).

Table 1. Overview over typical information required by the majority of context-aware office applications

Type	Description
Identity Information	The identification of a specific user represents the initial step for all personalized services. From a technical point of view it is not necessary that users reveal their 'real' identity. Instead, pseudonyms can be used for the identification process and personal information can be stored in anonymous profiles.
Location Information	Of all context information, which is available in real-world environments, the users' location is still the information type most often used in context-aware applications. The majority of systems uses RFID technology as a low-cost solution to simultaneously capture location and identity information.
Activity Information	Activity information can be either data about past and current tasks or long-term activities, usually referring to specific projects or responsibilities within the company. Some applications also include up-to-date information about the current work status or progress of specific tasks.
Availability Information	Making assertions about the availability of a certain person usually requires the combination of different types of information. In workplace environments, for example, availability information could be derived by interrelating information about the presence of a user and his current activity.
Biometric Information	In general, biometric information includes a variety of different data types. Regarding the functionalities described in the scenario elements, biometric information was mostly reduced to data about the current mood or stress level of a user.
Personal Preferences	In the context of smart office environments, personal preferences incorporate different types of information from various areas of everyday life. Personal preferences range from very private information, which is usually not available to co-workers (like, e.g., personal interest) to shared workplace information, which could be easily perceived by most colleagues in a shared work environment (for example the preferred room temperature or lightning).
Agenda Information	Information gained from personal calendars, agendas or task lists are necessary to predict up-coming activities and events. In addition, knowledge about existing personal appointments is necessary to enable automatic meeting planning among multiple users.

3.2 Data Capturing Mechanisms

When looking at context-aware services, it becomes obvious, that designers have different views about the level of control, which users should have over these services. Although the degree of system support could be adapted in numerous steps, it seems useful to distinguish between three general approaches: autonomous, user-approved and user-controlled services. Table 2 briefly describes the different concepts.

Table 2. Different levels of control over context-aware services

Control	Description
Autonomous Action	Autonomous services provide the lowest degree of user control. Processes are fully automated and users do not have a chance to control (e.g., acknowledge or reject) the functionality that is provided. In most cases, the service is automatically provided as soon as the user is identified by the system or a special event occurs (e.g., a user reaches a specific location).
User-Approved Action	Unlike autonomous services, user-approved services are not providing any functionality, unless the user approves it. Instead, the system fulfills an auxiliary role and acts in form of a digital assistant, which offers functionalities that might be helpful for the user in his current situation.
User-Controlled Action	In user-controlled services users maintain the full control over the service and can decide when and where a certain service is provided. In contrast to functionalities, provided by traditional computer systems, the provided services are mostly personalized and adapted to the current context of the user.

Similar to personalized user services, the collection of context information allows considerable variability in its degree of automation. While fully automated capturing mechanisms seem to be preferable at first sight, several studies, e.g., [34] showed, that users often feel uneasy if they are not in control over the data collection process. Therefore, it is important to test the users' willingness to provide personal information with respect to different data capturing mechanisms. The previous distinction between autonomous, user-approved and user-controlled services proved to be useful for the majority of 'high-level' services, where users gain concrete benefits from the usage of a certain application or system. With regard to the collection of context information, a distinction between user-approved and user-controlled mechanisms is not required as no direct service is provided to the user. For the purpose of the user study only two possible ways for the collection of context information are considered:

- **Automated Capturing:** The required information is continuously collected by the system. While there is not effort required from the user, the control over when and where personal data is being captured is very limited.
- **Individual Control:** The information being provided to the system can be individually controlled by the user. While this increases in the degree of control over the flow of personal data, it requires continuous effort from the user.

As the acceptance of the different data collection mechanisms is expected to depend on the type of information that is being collected, the preferred level of control over the data collection process is individually tested for each information type.

3.3 Inter-personal and Inter-cultural Differences

As stated earlier, the users' personal and cultural background is the third factor, which is expected to influence the willingness to provide individual context information. Prior to the investigation of potential correlations, existing technology adoption studies were reviewed to identify relevant personal characteristics. The following sections briefly discuss the different characteristics, which showed significant differences in previous evaluations and which will therefore be addressed in the user study.

Gender. Several studies explored the effect of gender on the adoption of different technologies and found significant differences between men and women. For example, Gefen and Straub [17] studied gender differences in the perception and use of e-mail and found, that gender had a significant impact on the perceived ease of use and usefulness. Studying technology usage decisions, Venkatesh and Morris [37] found, that the decision of women to use a specific technology is mostly influenced by the perceived ease of use, while those of men were strongly influenced by their perceptions of usefulness.

Age. The implementation of new technologies in workspaces is often accompanied by a change in existing work practices [30]. Over the last decades, a variety of studies found substantial evidence, which indicates that older workers tend to resist technological changes and avoid adopting new technologies [10]. There exist several attempts to explain, why age negatively affects technology adoption. One possible explanation is computer knowledge, which many older workers lack in comparison with their younger colleagues (see, e.g., [2]). So, even if older employees might be willing to adopt new technologies, they are likely to find it more difficult to actually use these technologies [18]. This might be supported by the fact, that cognitive skills decrease as people get older [7]. Another fact, that might contribute are personal habits and routines, which become stronger in age, and are therefore more difficult to change [20]. Nevertheless, there are also some studies, which found a positive correlation between age and adoption behavior. For example, Rai and Howard [29] studied the adoption of computer-aided software engineering tools and found, that age is positively related with adoption. One possible explanation is, that older professionals with more years of experience are more likely to perceive the benefits of new technologies [28].

Computer Literacy. Empirical evidence suggests, that there is a positive correlation between computer literacy and computer usage for traditional computer systems. For example, Alshare et al. [3] found, that computer literacy is a significant factor affecting the usage of computers by students. Based on this observation they conclude, that once users become more computer literate, they tend to develop a positive attitude and perceive computers as helpful tools, which are easy to use. The same behavior is likely to be true for context-aware systems, and users with more knowledge about computers and technology in general are more likely to adopt the new functionalities. But computer literacy in general is hard to quantify, and a variety of

different definitions and measurements have been used in the past. Following the approach of Alshare et al. [3], two different measures for computer literacy are used in this paper: the duration of computer usage per day and the participants' individual assessment of their personal computer knowledge.

Educational Level. Similar to computer literacy, several studies (see, e.g., [35]) suggest, that the education of a user is positively related to the adoption of new technologies. Burton-Jones and Hubona [10] investigated the adoption behavior of new e-mail and word processing applications and found, that the educational level directly effects the usage of the application. Again, there are several theories to explain this correlation. In general, a higher educational level is likely to reduce anxiety [22], and at the same time enables users to better judge the benefits of new technologies [2]. In addition, the educational level of users generally reflects their internal capabilities, such as technical skills and intelligence [25], which in turn enables more effective learning [4].

Nationality. As culture has a significant impact on organizational theories (see, e.g., [21]), Mao and Palvia [24] argue, that it would be erroneous to assume that new technologies are accepted equally well in different cultural settings. One recent example for cultural differences in adoption process of new technologies are mobile internet applications. For example in Japan, the i-mode system attracted more than ten thousand new customers per day, after it was introduced in 2001 [26]. In June 2002, the system was launched in Taiwan, and by May 2003 more than 900.000 users subscribed to the service [5]. In contrast, most mobile phone customers in Europe and the US are still not using the technology, although mobile internet applications have been introduced several years ago and are widely available today. And also regarding the protection of personal data, inter-cultural differences seem to exist. For example, Cvrcek et al. [14] found that Greek participants rated location privacy significantly higher than participants from other European countries.

Other Factors. Besides the individual user differences illustrated above, there are several other factors that might have an influence on the willingness to provide information and the acceptance of the different capturing mechanisms. Especially in group situations, the relation to colleagues as well as the general trust towards the company might have considerable effects on both aspects. A variety of studies (see, e.g., [12] or [13]) showed, that the climate within a company and its corporate culture can significantly effect organizational innovations. Although these factors are important, they are rather difficult to incorporate in a user study, as objective and reliable measures are very difficult to determine. Therefore, these factors will not be evaluated in the context of this paper.

4 Evaluation

4.1 Evaluation Scenario

As illustrated above, the this paper aims to analyze the general willingness of users to share context information in technology-enhanced work environments, in order to identify essential user requirements regarding the design of future office systems. In

the past, the majority of evaluations concentrated on individual services and specific system prototypes. Consequently, the insights gained in these evaluations, are mostly application and technology specific, and therefore have only limited validity when it comes to the design of new applications. Generalizing the findings obtained in these evaluations might result in misleading conclusion. For example, the rejection of personalized and context-adapted information presentation in multi-user applications does not necessarily mean, that such services would not be appreciated by the same group of users in an individual work situation. So while it is of particular importance to abstract from specific technologies and concrete or singular application situations, experiences in the past also showed, that individuals tend to overrate their privacy sensitiveness if questions are posed out of the context of a specific application or service (see, e.g., [11], [19] or [36]).

To counteract the apparent dichotomy [1] between privacy attitudes and actual behavior, without neglecting the overall research goal, a scenario-based evaluation approach was chosen. Instead of evaluating a particular prototype, a group of systematically constructed scenario elements was used for the study. This enabled participants to assess generic functionalities of context-aware applications, independent from the underlying technologies, interfaces and visualizations techniques, and guaranteed, that the feedback, gained from potential users, is not influenced by the way the functionalities or user services are implemented. At the same time, presenting a descriptive scenario prior to the actual evaluation process assures, that the concerns associated with the collection of personal information and weighted against the potential benefits of context-aware systems.

Before defining the test scenario, existing applications and usage situations were analyzed in order to identify representative functionalities of future office systems. Altogether, N=516 scenario elements coming from 68 different literature sources were examined. In the course of the analysis 39 different types of functionalities were identified, which could be clustered into 6 application areas (see [31] for more details). Looking at the frequency distribution of the different functionalities revealed, that the 8 most implemented functionalities cover approximately 44% of all analyzed scenarios. To ensure that the evaluation scenario remains understandable for a broad user population, it was decided to concentrate on those 8 functionalities and incorporate them into a coherent storyline, describing a working day of two knowledge workers in a technology-enhanced office environment.

4.2 Materials and Methods

The scenario was presented to participants using a questionnaire. In the first part of the questionnaire the evaluation scenario was presented and the different data collection mechanisms were explained. The participants were then asked to assess their willingness to provide different types of information, necessary to provide the functionalities illustrated in the scenario. For each of the seven information types, automated as well as user-controlled capturing mechanisms had to be assessed individually on 10-point rating scales. Prior to the assessment, an example question was shown in order to illustrate how the feedback scales should be used.

4.3 Participants and Evaluation Schedule

In order to identify inter-cultural differences, participants from Germany and the United States were involved in equal parts. For each country, N=100 paper-based questionnaires were personally given out to participants with work experience in office environments. In total, N=161 persons returned their questionnaire, which resembles a return rate of 80,5%. Out of this group, N=95 came from Germany and N=65 from the United States. The overall population (see Table 3) was nearly evenly distributed over male (49,1%) and female participants (50,9%), with slightly more males (52,1%) in Germany and slightly more female participants (55,4%) in the United States. While the American participants were nearly equally dispersed over the three age groups, most of the German participants (42,7%) were between 30 and 39 years old, followed by the group of 40-years-old and older (38,5%). The degree of computer literacy seems to be higher for the American participants, reflected by longer hours of computer usage per day and a higher level of self-assessed computer knowledge. Over 84% of the American participants use computers for more than 3 hours per day, compared to 61,5% of the German participants. Regarding their level of computer knowledge, nearly half of all American participants (49,2%) rate their knowledge as 'excellent', while this is only the case for 11,5% of the German participants. The educational level of the American participants is slightly higher, with 60% of the participants holding a master's or doctoral degree and only 1 participant with a high school degree.

5 Results

5.1 Willingness to Provide Context Information

As explained above, the participants were asked to state their willingness to provide different types of personal information, depending on the level of control they have over the data collection process. A value of '0' on a 10-point scale means, that a participant is absolutely not willing to provide the corresponding information, while a '10' indicates, that he would undoubtedly provide this information. Table 3 gives an overview over the willingness to provide personal information if the data collection process is controlled by the system. The mean values (M) and standard deviations (SD) are separately shown for German and American participants as well as the overall group.

An average overall willingness of M=3,49 shows, that the participants are quite reserved regarding the usage of automated capturing mechanisms. Looking at the national mean values reveals a considerable difference between the German and American group. With an average mean value of M=4,89 the willingness of American participants to provide context information is nearly twice as high as the willingness of German participants (M=2,55). With ratings smaller than 5 for all types of information, there is a tendency of German participants rather not to provide any context information if the data capturing process can not be controlled by the user. Although the willingness of American participants is higher for all information types, only 3 out of 7 ratings are above 5.

Table 3. Willingness to provide personal information if the data collection process is controlled by the system

	Germany		USA		Overall	
Type of Information	**M**	**SD**	**M**	**SD**	**M**	**SD**
1. Identity Information	4,35	3,49	5,61	2,77	4,86	3,27
2. Location Information	2,28	2,65	4,94	3,47	3,35	3,27
3. Activity Information	1,91	2,51	3,95	3,41	2,73	3.07
4. Availability Information	2,95	3,02	5,39	3,21	3,94	3,32
5. Biometric Information	1,24	1,62	3,27	3,29	2,06	2,62
6. Personal Preferences	2,17	2,77	6,36	3,23	3,85	3,60
7. Agenda Information	2,97	2,77	4,68	3,17	3,66	3,05
Average Willingness	**2,55**		**4,89**		**3,49**	

In all three groups biometric information got the lowest rating with a mean value of only M=1,24 in the German sub-group. This is followed by information about the current activity of a user with an overall mean value of M=2,73. The information type, which received the highest rating is identity information. With an overall mean value of M=4,86, the participants are more than two times more willing to provide information about their identity than information about their current physiological state (M=2,06). The ratings of the remaining four information types differ between the German and American sub-groups. While the difference is usually only one rank, there are considerable differences regarding the willingness to provide information about personal preferences. With a mean value of M=6,36 American participants are nearly three times more willing to provide personal preference information than German participants (M=2,17).

Table 4. Willingness to provide personal information if the data collection process is controlled by the user

	Germany		USA		Overall	
Type of Information	**M**	**SD**	**M**	**SD**	**M**	**SD**
1. Identity Information	7,21	2,61	8,14	1,76	7,59	2,34
2. Location Information	6,24	3,36	7,94	1,91	6,93	2,98
3. Activity Information	5,67	3,23	7,30	2,07	6,32	2,92
4. Availability Information	7,08	2,63	8,20	1,97	7,53	2,44
5. Biometric Information	2,47	2,52	4,98	3,65	3,47	3,26
6. Personal Preferences	4,89	3,09	7,70	2,65	6,02	3,22
7. Agenda Information	6,33	2,77	7,80	1,85	6,92	2,54
Average Willingness	**5,70**		**7,44**		**6,40**	

For all three groups the average willingness to provide personal information is higher, when the data collection process can be individually controlled by the user (see Table 4). Similar to the previous situation, biometric information received the lowest rating of all information types with an overall mean value of M=3,47. The participants are most willing to provide information about identity and current availability.

A detailed comparison between automated and user-controlled capturing methods is done in the next section.

5.2 Influence of the Level of Control on the Willingness to Provide Information

An overview over the influence of the level of control on the willingness to provide context information is shown in Table 5. Two-tailed t-tests were computed for all questionnaire items to compare the mean values between the different capturing mechanisms. For each information type, the mean difference (MD) and significance level are presented separately for both sub-groups as well as for the overall group. The p-values were calculated up to three positions after the decimal point, p-values smaller than that are shown as '0,000', which means that the difference is significant on a level smaller than p=0,0005.

Table 5. Overview of the influences of the level of control on the willingness to provide personal information

	Germany		**USA**		**Overall**	
	MD	**Sig.**	**MD**	**Sig.**	**MD**	**Sig.**
1. Identity Information	-2,8589	0,000	-2,5262	0,000	-2,7238	0,000
2. Location Information	-3,9542	0,000	-2,9687	0,000	-3,5600	0,000
3. Activity Information	-3,7573	0,000	-3,3431	0,000	-3,5901	0,000
4. Availability Information	-4,1250	0,000	-2,8108	0,000	-3,5944	0,000
5. Biometric Information	-1,2323	0,000	-1,7516	0,001	-1,4400	0,000
6. Personal Preferences	-2,7229	0,000	-1,3438	0,010	-2,1712	0,000
7. Agenda Information	-3,3594	0,000	-3,1250	0,000	-3,2656	0,000

The results show that the tested data capturing mechanisms have a considerable influence on the participants' willingness to provide context information. For all three groups the level of control has a highly significant effect on all of the seven tested information types. The table also shows that all mean differences are negative, which means, that the rating of the second question, describing individual control mechanisms, is higher for all types of information. The biggest variation in mean differences is observable in the German sub-group, with differences ranging from MD=-1,2323 for biometric information to MD=-4,1250 for availability information.

5.3 Analysis of Individual Differences

The differences regarding the influence of the various personal characteristics on the willingness to provide context information are illustrated in Table 6. The participants'

nationality seems to be the most influencing factor regarding the willingness to provide context information. For all 14 questions there are significant differences (5%-level) between the answers provided by German and American participants. In nearly 80% of the cases the differences are still significant on a 0,1%-level. The participants' self-assessed computer knowledge is another factor that seems to have a relatively strong influence on the willingness to provide context information. Nearly two third of the questions show significant differences between the answers provided by participants with different degrees of computer knowledge. For 8 of the 14 questions the differences are even significant on a 1%-level. The influence of the remaining four factors is considerably lower. With significant differences in the responses of three (age and computer usage per day) respectively four questions (gender and education), only one forth of the questions show significant effect on the willingness to provide context information.

Table 6. Overview over the influences of inter-personal differences on the willingness to provide context information

	Items with p≤0,05		**Items with p≤0,01**		**Items with p≤0,001**	
	Freq.	**Perc.**	**Freq.**	**Perc.**	**Freq.**	**Perc.**
Nationality	14	100,0%	12	85,7%	11	78,6%
Gender	4	28,6%	2	14,3%	2	14,3%
Age	3	21,4%	2	14,3%	1	7,1%
Computer Usage per Day	3	21,4%	1	7,1%	0	0,0%
Computer Knowledge	9	64,3%	8	57,1%	2	14,3%
Education	4	28,6%	3	21,4%	2	14,3%

As illustrated above, American participants are generally more willing to provide personal information, independent of the information type and the way the information is collected. One possible explanation for these obvious differences might be the general awareness about the potential consequences of data misuse. Compared to the United States most European countries have strict data protection laws, which prohibit unnecessary collection and storage of personal data. The violation of these laws is mostly accompanied by extensive media coverage, which might increase the valuation of personal information privacy within the German society. In addition, American participants are much more used to the disclosure of personal information in everyday life. For example, personalized bonus or pay back cards have a long tradition in the American consumer world. In Germany such bonus systems are relatively new and the willingness of the consumers, to disclose their personal shopping behavior in order to receive a discount on their purchases, is still quite low. Both aspects might contribute to the apparently higher comfort level of American participants to disclose data about personal interests and habits to co-workers or superiors.

Another explanation might be a confundation of the participants' nationality and their computer literacy. As shown in Table 6, the participants' self-assessed computer knowledge has a rather strong influence in the willingness to provide personal information. Looking back at section 4.3 shows, that nearly half of all American

participants (49,2%) rated their computer knowledge as 'excellent', while this is only the case for 11,5% of the German participants. With a mean value of M=4,22 on a 5-point scale the self-assessed computer knowledge is considerably higher in the American group compared to the German group with an average rating of M=3,15. Hence, it is possible that the large influence of the participant's nationality is not only caused by cultural differences, but also by dissimilarities in the level of computer knowledge between German and American participants.

6 Conclusion and Future Work

The results of the study show that potential users are rather reluctant to provide context information, especially if the data is automatically captured by the system. However, the personalization of context-sensitive applications will always require, that the system is aware of the personal preferences of the individual user as well as the current context in which the service is provided. This discrepancy between technical necessities and user preferences is likely to lead to considerable acceptance problems when installing context-aware systems in work environments.

The study also shows, that there seem to be different requirements regarding the protection of private data between users with different cultural backgrounds. The analysis of inter-personal differences shows, that the willingness to provide personal information differs enormously between German and American participants. In this context, the results of this study are inline with the findings by Cvrcek et al. [14], who found significant differences regarding the valuation of location data among participants from different European countries. In addition, the level of self-assessed computer knowledge has significant influences on at least one third of all questionnaire items. This shows that there are considerable differences regarding the design requirements of context-aware applications between user groups with different cultural backgrounds and different degrees of computer knowledge.

The information types used in this study represent only a very limited selection of information, which is usually available to co-workers in a shared work environment. In order to develop successful applications it is important to know, if general characteristics exist, which determine whether a certain type of information is freely provided or not. The evaluation showed considerable differences among the various types of information. Nevertheless, the data tested in this paper are not sufficient to clearly determine the characteristics, which influence the user's willingness to provide certain types of information. For example, it seems as if users are quite willing to provide information, which is visible to others in shared work environment (e.g., identity information), while information that is usually not visible to others (e.g., the current physiological state), is only reluctantly provided. However, this hypothesis does not hold true for all types of information. For instance, the participants were rather hesitant to provide activity data, even if employees are typically aware of the current activities of their colleagues. Therefore, further studies with additional information types are necessary in order to get a broader data basis, which enables the definition of higher-level design guidelines.

References

1. Acquisti, A., Grossklags, J.: Privacy and Rationality in Individual Decision Making. IEEE Security and Privacy 3(1), 26–33 (2005)
2. Agarwal, R., Prasad, J.: Are Individual Differences Germane to the Acceptance of New Information Technologies? Decision Sciences 30(2), 361–391 (1999)
3. Alshare, K., Grandon, E., Miller, D.: Antecedents of Computer Technology Usage: Considerations of the Technology Acceptance Model in the Academic Environment. Journal of Computing Sciences in Colleges 19(4), 164–180 (2004)
4. Ashcraft, M.H.: Cognition. Prentice Hall, Upper Saddle River (2002)
5. Barnes, S.J., Huff, S.L.: Rising Sun: iMode and The Wireless Internet. Communications of the ACM 46(11), 78–84 (2003)
6. Benham, H.C., Raymond, B.C.: Information Technology Adoption: Evidence from a Voice Mail Introduction. ACM SIGCPR Computer Personnel 17(1), 3–25 (1996)
7. Brigman, S., Cherry, K.E.: Age and Skilled Performance: Contributions of Working Memory and Processing Speed. Brain and Cognition 50, 242–256 (2002)
8. Brynjolfsson, E.: The Productivity Paradox of Information Technology. Communications of the ACM 36(12), 66–77 (1993)
9. Brynjolfsson, E., Hitt, L.: Paradox Lost? Firm-Level Evidence on the Returns to Information Systems Spending. Management Science 42(4), 541–558 (1996)
10. Burton-Jones, A., Hubona, G.: Individual Differences and Usage Behavior: Revisiting a Technology Acceptance Model Assumption. ACM SIGMIS Database 36(2), 58–77 (2005)
11. Chellappa, R.K., Sin, R.: Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Inform. Techn. and Management 6(2-3), 181–202 (2005)
12. Cooper, R.B.: The Inertial Impact of Culture on IT Implementation. Information & Management 27(1), 17–31 (1994)
13. Cooper, R.B., Zmud, R.W.: Information Technology Implementation Research: A Technological Diffusion Approach. Management Science 36(2), 123–139 (1990)
14. Cvrcek, D., Kumpost, M., Matyas, V., Danezis, G.: A Study on the Value of Location Privacy. In: Proc. of the Fifth Workshop on Privacy in the Electronic Society, pp. 109–118 (2006)
15. Dewan, S., Min, C.: The Substitution of Information Technology for Other Factors of Production: A Firm Level Analysis. Management Science 43(12), 1660–1675 (1997)
16. Friedewald, M., Vildjiounaite, E., Wright, D.: The Brave New World of Ambient Intelligence: A State-of-the-Art Review. Deliverable D1 of the SWAMI consortium to the European Commission under contract 006507 (2006)
17. Gefen, D., Straub, D.: Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model. MIS Quarterly 21(4), 389–400 (1997)
18. Gomez, L.M., Egan, D.E., Bowers, C.: Learning to Use a Text Editor: Some Learner Characteristics that Predict Success. Human Computer Interaction 2, 1–23 (1986)
19. Hann, I.-H., Hui, K.-L., Lee, T.S., Png, I.P.L.: The Value of Online Information Privacy: Evidence from the USA and Singapore. Paper presented at the International Conference on Information Systems (2002)
20. Harrison, A.W., Rainer, R.K.: The Influence of Individual Differences on Skill in End-User Computing. Journal of Management Information Systems 9(1), 93–111 (1992)
21. Hofstede, G.: Culture's Consequences – Comparing Values, 2nd edn. Institutions and Organizations Across Nations. Sage, London (2001)
22. Igbaria, M., Parsuraman, S.: A Path Analytic Study of Individual Characteristics, Computer Anxiety, and Attitudes Towards Microcomputers. Journal of Management 15(3), 373–388 (1989)

23. Lahlou, S., Langheinrich, M., Röcker, C.: Privacy and Trust Issues with Invisible Computers. Communications of the ACM 48(3), 59–60 (2005)
24. Mao, E., Palvia, P.: Testing an Extended Model of IT Acceptance in the Chinese Cultural Context. ACM SIGMIS Database 37(2-3), 20–32 (2006)
25. Mathieson, K., Peacock, E., Chin, W.W.: Extending the Technology Acceptance Model: The Influence of Perceived User Resources. The DATA BASE for Advances in Information Systems 32(3), 86–112 (2001)
26. Mattern, F.: Ubiquitous Computing: Scenarios From an Informatised World. In: Zerdick, A., et al. (eds.) E-Merging Media – Communication and the Media Economy of the Future, pp. 145–163. Springer, Heidelberg (2005)
27. Pearson, J.M., Crosby, L., Bahmanziari, T., Conrad, E.: An Empirical Investigation into the Relationship between Organizational Culture and Computer Efficacy as Moderated by Age and Gender. Journal of Computer Information Systems 43(2), 58–70 (2002)
28. Prescott, M.B., Conger, S.A.: Information Technology Innovations: A Classification by IT Locus of Impact and Research Approach. ACM SIGMIS Database Archive 26(2-3), 20–41 (1995) Special Double Issue: Diffusion of Technological Innovation
29. Rai, A., Howard, G.S.: Propagating CASE Usage for Software Development: An Empirical Investigation of Key Organizational Correlates. OMEGA: The International Journal of Management Science 22(2), 133–247 (1994)
30. Robey, D., Sahay, S.: Transforming Work through Information Technology: A Comparative Case Study of Geographic Information Systems in County Government. Information Systems Research 7(1), 93–110 (1996)
31. Röcker, C.: Services and Applications for Smart Office Environments - A Survey of State-of-the-Art Usage Scenarios. Paper submitted to: International Conference on Computer and Information Technology (ICCIT 2010), Cape Town, South Africa, January 27-29 (2010) (submitted)
32. Röcker, C.: Ambient Intelligence in the Production and Retail Sector: Emerging Opportunities and Potential Pitfalls. In: Proceedings of the International Conference on Innovation, Management and Technology (ICIMT 2009), pp. 1393–1404 (2009)
33. Röcker, C.: Toward Smart Office Environments - Benefits and Drawbacks of Using Ambient Intelligence Technologies in Knowledge-Based Enterprises. In: Proc. of the Intern. Conference on Economics, Business, Management and Marketing (EBMM 2009), pp. 17–21 (2009)
34. Röcker, C., Janse, M., Portolan, N., Streitz, N.A.: User Requirements for Intelligent Home Environments: A Scenario-Driven Approach and Empirical Cross-Cultural Study. In: Proceedings of the International Conference on Smart Objects & Ambient Intelligence (sOc-EUSAI 2005), Grenoble, France, October 12 - 14, pp. 111–116 (2005)
35. Russo, N.L., Kumar, K.: Studying the Impact of Information Technology Innovations in Organizations: The Influence of Individual Characteristics, Innovation Characteristics, and the Innovation Introduction Process. In: Kendall, K.E., et al. (eds.) The Impact of Computer-Supported Technologies on Information Systems Development. Elsevier Science Publications, Minneapolis (1992)
36. Spiekermann, S., Grossklags, J., Berendt, B.: E-Privacy in Second Generation E-Commerce: Privacy Preferences versus Actual Behavior. In: Proceedings of the ACM Conference on Electronic Commerce (EC 2001), pp. 38–47. ACM Press, New York (2001)
37. Venkatesh, V., Morris, M.: Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and their Role in Technology Acceptance and Usage Behavior. MIS Quarterly 24(1), 115–139 (2000)

Implementation and Evaluation of Agent Interoperability Mechanism among Heterogeneous Agent Platforms for Symbiotic Computing

Takahiro Uchiya[1], Susumu Konno[2], and Tetsuo Kinoshita[3]

[1] Nagoya Institute of Technology,
Gokiso-chou, Showa-ku, Nagoya, 466-8555 Japan
[2] Chiba Institute of Technology,
2-17-1 Tsudanuma, Narashino, 275-0016 Japan
[3] Tohoku University
2-1-1 Katahira, Aoba-ku, Sendai, 980-8577 Japan
t-uchiya@nitech.ac.jp, konno.susumu@it-chiba.ac.jp
kino@riec.tohoku.ac.jp

Abstract. An "Agent Platform" is a framework that supports and facilitates intelligent operations. In this study, we particularly address interoperability among agents situated in different agent platforms. This paper presents a proposal of a flexible interoperability mechanism among heterogeneous agents, which enables efficient development and maintenance processes of agent systems. Furthermore, we present results of experiments to underscore the effectiveness of the proposed method.

Keywords: Agent interoperability mechanism; Symbiotic Computing.

1 Introduction

Using recent Information and Communication Technology (ICT), people can obtain much information from digital spaces (DSs) such as the internet. Useful workspaces or communities can be constructed in a DS as well in a real space (RS) in the physical world. In fact, ICT transforms traditional society into modern networked societies in which people can exchange information and knowledge freely and easily. However, emerging problems are becoming apparent in internet society such as the digital divide/e-Gap, security, and network-based crimes. Modern ICT should confront these difficult problems and provide solutions by bringing sociality and humanity into computing models. Based on cognitive informatics [1], a model of cognitive properties to bring human factors and social relations into information processing was proposed and discussed by Wang and Kinsner [2][3].

To overcome these problems, *Symbiotic Computing*, which we have proposed, provides a framework to bridge an e-Gap between RS and DS [4][5]. We consider that the e-Gap, from which problems arise, results from a lack of mutual cognition between RS and DS: people cannot receive advanced services without IT skills.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 107–118, 2010.

Consequently, DS cannot provide a service that is suitable for users depending on their respective situations and preferences. Moreover, DS cannot provide a safe and secure service without heuristics related to a person's activities in a society, such as customs, norms, and expertise.

In our framework, agent-based design models of both the symbiotic function (SF) and the symbiotic application system (SAS), which consists of many SFs that support various activities of people, are adopted based on agent-based computing technologies. An SAS operates in an open distributed environment in which RS and DS fluctuate from time to time and provide stable services for people. Therefore, the SAS must deal with such fluctuations autonomously by tuning and changing its structure and functions. The necessary properties of an SAS—intelligence, flexibility, and adaptability—can be realized easily by composing the SAS as an "Agent System" [6]. As described in this paper, we specifically examine agent and multiagent technologies for building an SAS over an open distributed environment.

Recently, many agent platforms have been developed to facilitate multiagent activities and coordination. However, each agent platform is developed to solve a specific problem in a certain problem domain. Consequently, each platform has a different specialty. This study proposes and implements a flexible interoperability mechanism among heterogeneous agents, which enables efficient development and maintenance processes of agent systems. Legacy resources can be reused as well because of the existence of the interoperability functionality.

2 Related Works

2.1 Agent Platforms

An agent platform is an execution environment for agents. It supports agent activities of all kinds, such as inter-agent communication functions, and coordination functions. Agent platforms are divisible approximately into two categories, **original specification agent platforms** and **FIPA-compliant agent platforms**.

[Original specification agent platforms]
An original specification agent platform is designed for a certain problem domain with special functionality. These platforms are classifiable into the following three categories: (A) mobile agent platforms, (B) intelligent agent platforms, and (C) dynamic self-organization platforms. This study specifically examines platforms of type (C). Dynamic self-organization platforms realize their purpose, which is to be a distributed flexible system that can do self-organization and reorganization of agents. Figure 1 shows that DASH [7] is one of this kind, as implemented with the concept of a repository-based agent framework.

The DASH agent platform comprises a workplace and agent repository. Agents situated in the agent repository will be organized autonomously to satisfy a user's requirement according to the user's request or other agents' request. An instance of the organization is created on the workplace as a multi-agent system. The whole process is conducted according to the organizational protocol provided by the DASH platform, whereas coordination among agents on the workplace is conducted by the coordination protocol provided by the DASH platform. We chose the DASH platform

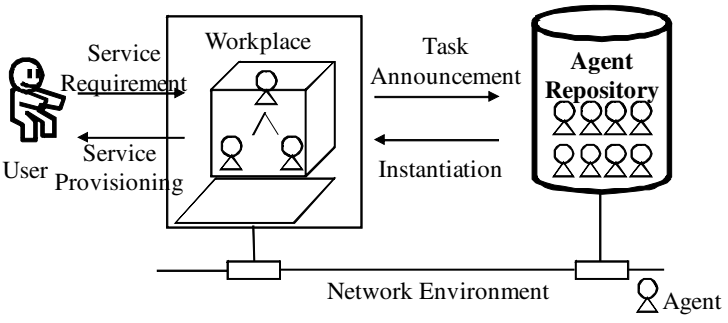


Fig. 1. DASH Agent Platform

as one platform in our experiments because these functions render the DASH platform capable of providing flexibility to react to distributed computing resource changes.

[FIPA-compliant agent platforms]
A FIPA-compliant agent platform is implemented in accordance with the specification suggested by FIPA, which is a standardization organization for agent technology and which mainly addresses specifications related to interoperability. By FIPA specification, an agent communication channel is responsible for communication among different platforms. The domain for the platform is an aggregation of agents that is managed by a directory facilitator. These agents can be situated and active in different platforms. The domain can also be recognized as a unit that composes applications. Such FIPA-compliant platforms are SAGE [8], JADE [9], etc. We chose SAGE for our experiments because of its fault tolerance, scalability, and excellent security. The SAGE agent is designed and implemented in Java language, so the SAGE agent is suitable for the performance of critical operations such as accessing and managing databases.

2.2 Related Works of Interoperability among Agent Platforms

The Agentcities Project [10] specifically examines interoperability among FIPA-compliant systems, but the original specification agent platform is not considered.

The study of the agent platform protocol [11] assesses interoperability between the FIPA-compliant platform and the original specification platform, but their realization methodology is based on platform modification, which means that modification of the connection module is needed every time that the system is upgraded or the architecture of the platform changes.

The study of the gateway agent [12] presents interoperability between the FIPA-compliant agent and the original specification agent by conversion of agent mental states, agent communication language, and message transportation. Communication at a conversational level is obtained. However, the difference in procedures in communication processes is not supported. For that reason, it remains insufficiently robust for real applications.

3 Heterogeneous Agent Interoperability Mechanism

3.1 Proposals of Interoperability among Heterogeneous Agent Platforms

In our research, we resolve a salient problem encountered in past related works and provide a practical solution to realize interoperability among heterogeneous agents without massive platform modification.

The following methods can be considered:

(T1) Modification of the agent platform
(T2) Implementation of interoperability as a plug-in function to the platform that can be installed to the system
(T3) Implementation of the interoperability function as agents working on each platform

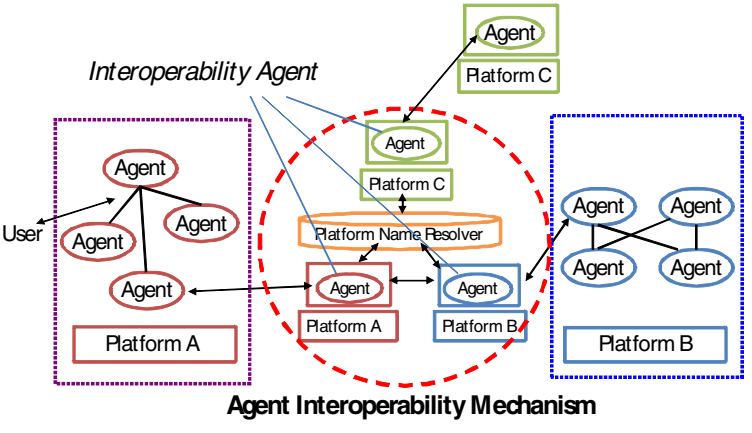


Fig. 2. Utilization of Interoperability Agent

For use in this study, after evaluating those three methods comprehensively, we chose (T3) for our implementation. An overview of this method is presented in Fig. 2.

3.2 Design

First, we checked the differences of the two platforms. They are the following:

[Agent Communication Language]
DASH uses ACL based on KQML; SAGE uses FIPA-ACL
[Agent Communication Protocol]
DASH is definable freely by developers; SAGE uses Interaction Protocol

Next, we defined the interoperability level as follows:

[Interoperability at the communication channel level]
This is for connection of two platforms.
[Interoperability at the message level], [Interoperability at the protocol level]
These are for absorption of differences of platforms.

[Interoperability at the practical level]
This is the supportive functionality for the cooperation of heterogeneous agents.

In this study, we take the **interoperability agent** approach to implement the proposed mechanism. Figure 3 depicts the internal structure of the proposed mechanism. In this mechanism, interoperability agents render it possible to realize interoperability at each previously described level. Finally, we designed the interoperability agent. Then, we describe the detail of the design.

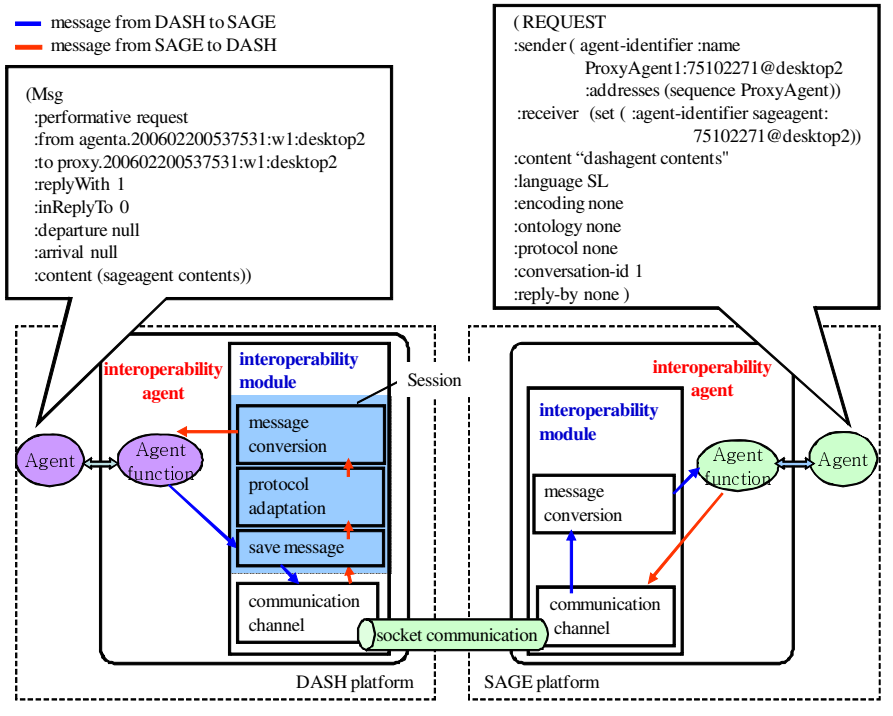


Fig. 3. Internal Structure of the Interoperability Module

(Design of the Communication Module)
To avoid modifying the platform, we use socket communication between platforms. In the DASH side, we implement a DASH proxy agent in Java (base process program), which is responsible for sending and receiving messages. In the SAGE side, a SAGE proxy agent is responsible for sending and receiving messages as well.

(Design of the Communication Language Conversion Module)
We implemented semantic message conversion to realize a conversation among heterogeneous agents that use different languages.

(Design of the Protocol Module)
The communication steps, the communication among platforms, must also follow the Interaction Protocol, which is a typical conversation pattern between agents.

In the DASH side, we must implement this Interaction Protocol by saving the continuous communication status into session information. The message sent to the DASH platform will be saved in session information first. Subsequently, according to the definitions of protocols, it will be decided whether to forward message to the DASH proxy agent or reply to the sender.

(Design of Platform Name Resolver)
To get information for peer platform location and to get information about the services provided by the peer platform, we designed a service lookup module using UDDI technology. This module comprises two parts—the UDDI registry and the UDDI client—which accesses the UDDI registry register service and search service.

3.3 Implementation

We implemented the proposed mechanism in Windows XP OS (Microsoft Corp.) using Java language. We created the DASH proxy agent on the DASH platform and SAGE proxy agent on the SAGE platform:

In the DASH side, the communication between the DASH agent and the SAGE agent is performed as follows through the interoperability module.

- Send message to DASH proxy agent
- After receiving the message, the DASH proxy agent will
  - Create a communication session, and save the received message to the session
  - Create a communication channel with SAGE
  - Convert the message format into FIPA-ACL
  - Send the message to the SAGE proxy agent at the SAGE platform
  - Get the reply message from the SAGE proxy agent at the SAGE platform
  - Save the received message to the session
  - Convert the saved message format used in the session by application of the protocol
- Forward the converted message to the target agent

In the SAGE side, the communication is performed as follows:

- Send message to SAGE proxy agent
- After receiving the message, the SAGE proxy agent performs the following procedure
  - Create a communication channel with DASH side
  - Send message to the DASH proxy agent
  - The SAGE proxy agent receives a reply from the DASH proxy agent
- The SAGE proxy agent forwards the message to the target agent

Regarding interoperability at a conversational level, to bridge the difference of FIPA-ACL and KQML, we apply the “session” concept, which is often used in the WWW domain. It helps to eliminate differences of the two agent communication languages.

Moreover, we implemented the communication mechanism among heterogeneous agents based on the “Interaction Protocol”. When the communication activity occurs, the message format conversion will be conducted as described below.

• Create session
• Save the communication message to the session
• Confirm the protocol that is used in the message if the necessary message will be forwarded to the target agent according to the "Interaction Protocol". Messages that are unnecessary for the agent will be deposited after they are received.

• Message format conversion. Three possibilities must be considered:

- Use a parameter when the parameter is semantically identical
- Set the parameter accordingly when semantics are identical
- Parameters that are only used in one platform will be set with initial values or set values according to the session information.

4 Experiment and Evaluation

4.1 Experiments

The experimental environment is the following:

Experiment computer 1 is Windows XP Service Pack 2 (Microsoft Corp.), Pentium 4 CPU 1.7 GHz (Intel Corp.), 1.00 GB RAM.
Experiment computer 2 is Windows XP Service Pack 2 (Microsoft Corp.), Pentium 4 CPU 2.4 GHz (Intel Corp.), 1.00 GB RAM.
The agent platform is the DASH agent platform and SAGE agent platform.

We executed three experiments to evaluate the interoperability mechanism.

•***[Experiment 1]*:** Testing and evaluation of the health diagnosis application using the proposed mechanism.
•***[Experiment 2]*:** Verification of the extensibility of proposed mechanism.
•***[Experiment 3]*:** Verification of the effectiveness of the proposed interoperability mechanism by comparing the workload of employed services provided by agents from other platforms through the proposed methodology, and the workload using the same services in the same platform.

[Experiment 1: Test and evaluation of the health diagnosis application using the proposed mechanism]
To verify the implemented interoperability mechanism's effectiveness and interoperability at the communication channel level, message level, and protocol level, we also implemented a health diagnosis support system using both merits of DASH and SAGE, with the proposed interoperability module.
The application outline is the following:

DASH platform: (Diagnosis function) Using an agent system with a reasoning function for diagnosis

SAGE platform:
(Manage the diagnosis result) Deposit and withdraw the diagnosis result to and from a database

(Search function) Search for the user's health diagnosis from the database and inform the health record to the user with the new diagnosis result or health suggestion. This health-diagnosis support system assists users by including the merits of the DASH platform and the SAGE platform, connected through the interoperability mechanism.

This system based on multi-agents with a reasoning function was implemented using the intelligent processing function of the DASH platform. By making full use of database access functionality of the SAGE platform, we implemented the function of storing users' health diagnosis information and the functionality of informing users with the past diagnosis information at the SAGE platform. The diagnosis support GUI is implemented on a DASH platform. Figure 4 depicts the scenario and how the system functions with the interoperability module.

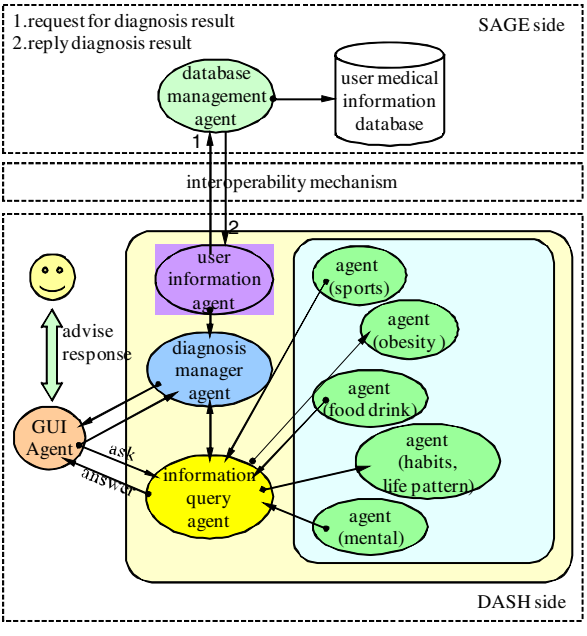


Fig. 4. Health Diagnosis System

In this system, the DASH GUI agent receives the input information from the user. It then retrieves all necessary information from the SAGE agent through the interoperability mechanism. Subsequently, with the knowledge that DASH has, the DASH agent conducts reasoning and produces a diagnosis and suggestions. It ultimately presents them to the user.

[Experiment 2: Verify the extensibility of the proposed mechanism]

To confirm the extensibility of the proposed interoperability mechanism, we added an interoperability module for another FIPA-compliant agent platform: JADE. Interoperability between the DASH and JADE platforms was also implemented.

[Experiment 3: Verification of the interoperability mechanism effectiveness]
We assume that a certain agent situated in one platform is trying to access the service provided by an agent situated in another different platform.

We compare the method of employing the service using the proposed interoperability module and a method of implementing the same service in the same platform. For the experiment, we executed a demonstration service of searching for hot springs using DASH agents.

4.2 Results and Evaluation

[Experiment 1]
Figure 5 shows screenshots of this experiment. The right panel portrays the screen of the DASH environment; the left panel shows the screen of the SAGE environment. Results of this experiment confirmed the functionality of the proposed mechanism at the communication channel level, the message level, and the protocol level according to the design from the result of the output and logging system. Moreover, we calculated the workload performed in the process of addition of the functionality. Table 1 presents the lines of source code that were written.

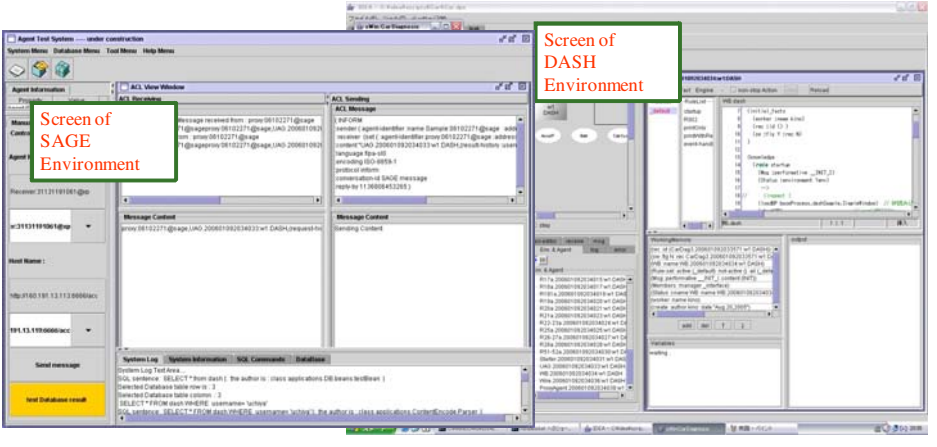


Fig. 5. Screenshots of Experiment 1

Table 1. Workload Comparisons in Experiment 1

	DASH function	SAGE function
Overall agents	46	2
Newly created agents	0	2
Number of source code lines [n]	2538	652
Newly written and modified lines [c]	72	652
Reused lines [n-c]	2466	-
Legacy source code reuse percentage [((n-c)/n) × 100]	97%	-

To add new functions to the SAGE platform, we newly added 652 lines of source code. In DASH, we added only 72 lines to the original lines to realize equivalent functionality. Therefore, the proposed configuration makes the re-usage rate close to 97%. Based on this result, we can infer that the effectiveness of the interoperability mechanism among heterogeneous agents is partially confirmed.

[Experiment 2]

Table 2 presents the necessary workload for adding the JADE interoperability module by reusing SAGE's source code. The operation that realizes the interoperability between DASH and JADE reused over 94% of the source code. The reusability for interoperability module is confirmed.

Table 2. Workload Comparisons in Experiment 2

	DASH	JADE
Number of source code lines [n]	1250	1664
Newly written and modified lines [c]	68	82
Reused lines [n-c]	1182	1582
Legacy source code reuse percentage [((n-c)/n) × 100]	94%	95%

[Experiment 3]

Table 3 presents two methods using services provided by agents situated in different platforms.

It is more efficient to use the proposed methodology to access the existing service than to implement the same service again. Simply taking quantities of the lines of the source code as a workload: 86% reduction can be made. According to this result, we can tell that the interoperability module is effective for applications in this domain.

Table 3. Workload Comparisons in Experiment 3

	Implement newly	Reuse through proposed mechanism
Number of total lines for source code	418	406
Newly coded and modified code lines	418 [M1]	62 [M2]
Re-used lines	0	344
Deduction rate of workload [((M1-M2)/M1) × 100]	-	86%

4.3 Discussion

In this study, we applied the proposed mechanism to platform DASH and SAGE. We confirmed the interoperability mechanism in a health-diagnosis support agent system. An operation verification experiment was conducted as well. The DASH side is responsible for autonomous intelligent diagnosis. The agent group performs diagnosis by coordinative information processing, whereas the SAGE side is responsible for managing a database system in which all users' medical data and diagnosis results are accumulated and stored. The SAGE side also serves diagnosis results or a user's past medical information to the DASH side when the DASH side requests it.

Experiments of accumulation and the retrieval of the medical data were conducted. The communication and the cooperation among agents functioned normally. Results proved that the proposed interoperability mechanism between the DASH and SAGE platform was effective.

5 Conclusion

We proposed and implemented the interoperability mechanism to realize interoperability among heterogeneous agents. Furthermore, we performed the verification and evaluation experiments and also confirmed that cooperation and coordination among heterogeneous agents through interoperability mechanisms is both possible and practical. Use of the interoperability mechanism and use of the existing service from the heterogeneous platform can be realized through rapid development with less coding.

Future work shall include the following. For this study, we implemented an interoperability mechanism on a DASH platform, a SAGE platform, and a JADE platform. We demonstrated the effectiveness of the mechanism using three experiments. However, for original specification agent platforms, we only implemented them on the DASH platform; platforms other than DASH must be verified. Moreover, we plan to carry out interoperability experiments using various agent platforms.

References

1. Wang, Y.: On Cognitive Informatics. In: Proc. 1st IEEE International Conference on Cognitive Informatics (ICCI 2002), pp. 34–42. IEEE CS Press, Los Alamitos (2002)
2. Wang, Y., Kinsner, W.: Recent Advances in Cognitive Informatics. IEEE Transactions on Systems, Man, and Cybernetics (C) 36(2), 121–123 (2006)
3. Wang, Y.: The Theoretical Framework of Cognitive Informatics. The International Journal of Cognitive Informatics and Natural Intelligence (IJCiNi) 1(1), 1–27 (2007)
4. Shiratori, N., et al.: Symbiotic Computing Project (2005), http://symbiotic.agent-town.com/
5. Suganuma, T., Uchiya, T., Konno, S., Kitagata, G., Hara, H., Fujita, S., Kinoshita, T., Sugawara, K., Shiratori, N.: Bridging the E-Gaps: Towards Post-Ubiquitous Computing. In: Proc. 20th International Conference on Advanced Information Networking and Applications (AINA 2006), FINA 2006 Symposium, vol. 2, pp. 780–784 (2006)
6. Sugawara, K., Fujita, S., Hara, H.: A Concept of Symbiotic Computing and its Application to Telework. In: Proc. 6th IEEE International Conference on Cognitive Informatics (ICCI 2007), pp. 302–311 (2007)

7. Fujita, S., Hara, H., Sugawara, K., Kinoshita, T., Shiratori, N.: Agent-based Design Model of Adaptive Distributed System. Applied Intelligence 9(1), 57–70 (1998)
8. Ghafoor, A., ur Rehman, M., Khan, Z.A., Farooq Ahmad, H., Ali, A., Suguri, H.: SAGE: Next Generation Multi-agent System. In: Proc. Parallel and Distributed Processing Techniques and Applications, pp. 139–145 (2004)
9. Bellifemine, F., Poggi, A., Rimassa, G.: JADE – A FIPA-compliant Agent Framework. In: Proc. Practical Application of Intelligent Agents and Multi Agents, pp. 97–108 (1999)
10. Agentcities project, http://www.agentcities.org/
11. Takahashi, K., Guoqiang, Z., Amamiya, S., Mine, T., Amamiya, M.: Message Communication Protocol for Interoperability between Agent Platforms. IEEJ Trans. on Electronics, Information and Systems 123-C (8), 1503–1510 (2003) (in Japanese)
12. Suguri, H., Kodama, E., Miyazaki, M., Kaji, I.: Assuring Interoperability between Heterogeneous Multi-Agent Systems with a Gateway Agent. In: IEEE International Symposium on High Assurance Systems Engineering, pp. 167–170 (2002)

B-Dash: Agent Platform for Mutual Cognition between Human and Agents

Hideki Hara, Yusuke Manabe, Susumu Konno,
Shigeru Fujita, and Kenji Sugawara

Chiba Institute of Technology, 2-17-1 Tsudanuma Narashino Chiba 275-0016, Japan
hara@net.it-chiba.ac.jp

Abstract. In this paper, we describe an agent-based platform called "B-DASH" for the Symbiotic Computing. Mutual cognition between human and agents is a key technology of the Symbiotic Computing. In order to promote that mutual cognition, B-DASH has a blackboard mechanism to integrate and share information.

1 Introduction

As the information technology is developed, it becomes increasingly easy to access many kinds of information resources. But many people cannot use them easily and safely because of remaining many barriers like digital divide and privacy issue.

To overcome these problems, we have proposed a concept of the Symbiotic Computing[3]. In this computing model, we use agent technology to bridge a gap between users and information resources.

To realize the symbiotic computing, mutual understanding between human and agent is required. In particular, it is important for agent to understand human behavior in order to provide appropriate service. Human behavior can be observed by using various sensors. However, to understand the behavior precisely and effectively, a mechanism for integrating and sharing sensor data is required.

We have developed agent-based software platform called "DASH"[5,2,1]. DASH is used to develop applications of the Symbiotic Computing. However using DASH system, it becomes difficult to develop the applications which use a number of information resources like sensor network. It is because DASH has no mechanism for integrating and sharing large amounts of data.

In this paper, we describe an agent-based platform called "B-DASH" for the Symbiotic Computing. B-DASH has a blackboard system to promote integrating and sharing a variety of information from sensors and agents.

2 Symbiotic Computing and Its Platform

2.1 Model of Symbiotic Computing

Symbiotic Computing is a technology to achieve a symbiosis between human in Real Space (RS) and ICT resources in Digital Space (DS). It is important that RS

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 119–127, 2010.

and DS understand each other to achieve the symbiosis. DS must collect a variety of information, knowledge and condition in RS like the environment info, users' info, etiquette, laws, local rules and task flows. On the other hand, RS must get the various specifications. For example, RS must have information about the architecture of systems, protocols, how to access to services. This mutual understanding will build the relation where RS and DS have any interactions as much as needed at the lowest cost when needed.

To realize such mutual understanding, we are designing a Symbiotic Platform shown in Fig. 1. This platform provides the functionality of autonomous behavior to DS. On this platform, some software called Perceptual ware and Social ware works for mutual understanding. Perceptual ware is software which receives various signals from various sensors. Using these signals, it observes human's behavior and the environment to understanding RS. Social ware is software to build a social model such as norms in society. It acquires various data from the Internet and human.

Perceptual ware and Social ware have to work autonomously. So, we decided to develop such software using the agent technology. There are two types of agent in our platform. Interface Agent works as an interface between the human and Perceptual/Social ware. Human can tell the explicit requirements to the symbiotic platform via Interface Agent. And the software working on the platform can also tell its requirement to human using Interface Agent. On the other hand, Cognitive agent is the software which works in the platform. It watches information from the sensors and infer the requirement of human. It also gets information from the web to search and provide appropriate information for human.

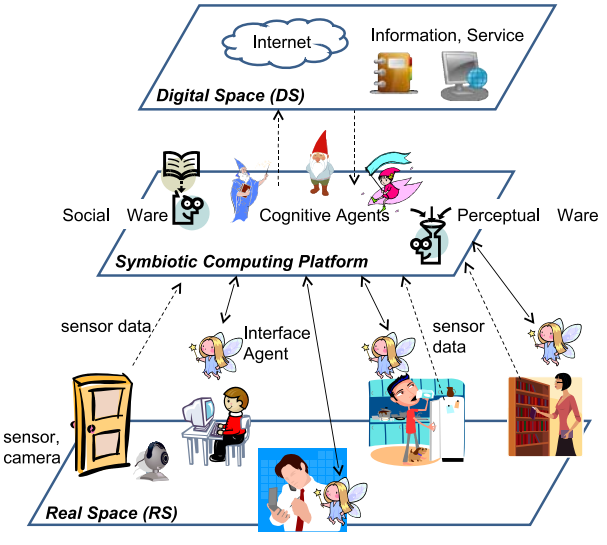


Fig. 1. Model of Symbiotic Computing

Using the symbiotic platform, we can achieve relationship of "mutual cognition" between RS and DS. So human can tell explicit or implicit requirements to DS as follows.

- Using Interface Agent, DS tells human what DS can do for human. So, human can understand what DS will do for human. As a result, human can tell his/her explicit requirement to DS appropriately.
- Using various sensor devices, DS observes human and infers the service or information which human really requires. So DS can understand implicit requirements of human. As a result, human can receive appropriate service/information from DS without difficult and complicated operations.

2.2 Requirements of the Symbiotic Platform for Mutual Cognition

On the symbiotic platform, several software systems called Perceptual/Social Ware work simultaneously for mutual cognition. They share various data from sensors to infer implicit requirement of human. And also they share the result of the inference. Functional requirements of the symbiotic platform where such software works are as follows.

(a) aggregation and sharing mechanism for information: Cognitive Agent infers behavior and intention using the data from sensors. To improve accuracy of the inference, Cognitive Agent has to use data from different types of sensors. So the symbiotic platform should be able to collect various data and to provide it to the agent. In addition, the platform should be able to provide the result introduced by an agent to another agent.

(b) communication mechanism for Interface Agent: Unlike Cognitive Agent, Interface Agent does not work on the symbiotic platform. It works on the machines like the user PC, web browser and cell phone. But Interface Agent has to share information which are used by Cognitive Agent in order to provide appropriate services to the user. So the platform should have functionality which supports communication between Interface Agent and Cognitive Agent.

3 B-Dash

3.1 Architecture of B-DASH

We developed a system called "B-DASH" for constructing the Symbiotic Computing Platform more easily. B-DASH system is an extended version of DASH system which is used for developing many agent-based applications. The features that are added to DASH system for the symbiotic platform are described as follows.

Blackboard module: Blackboard is used to hold and share various data. It stores data from the sensors and assumptions about human's behavior made by Cognitive Agent. Each Cognitive Agent shares data and assumptions using this blackboard.

Remote agent interface: This feature makes it easy to develop Interface Agents which communicate with Cognitive Agents. Using this interface, Interface Agents and Cognitive Agents can share data on the Blackboard. So these agents can communicate asynchronously.

Architecture of the B-DASH system is shown in Fig.2. The agents of B-DASH system work on user PCs and platforms for agents called "Workplace" and "Repository"

Workplace is an execution environment for the Cognitive Agents. It has a blackboard watched by the Cognitive Agents. Data from sensors are written in the blackboard as signal and then the cognitive agents infer behavior/intention of human using these signals. Several cognitive agents work cooperatively and write behavior/intension on the blackboard as assumptions.

Repository is a mechanism for persistent activity of agents and contents written on the blackboard. When the platform was stopped for some reasons, agents and contents on the blackboard are saved into the repository. They are reloaded into the workplace when workplace restarts.

On the user PCs, agents called Interface Agent works. It receives explicit requirement about services from user and provides services to user. Interface Agent also watches the PC and applications running on the PC to acquire user's implicit requirement and intention.

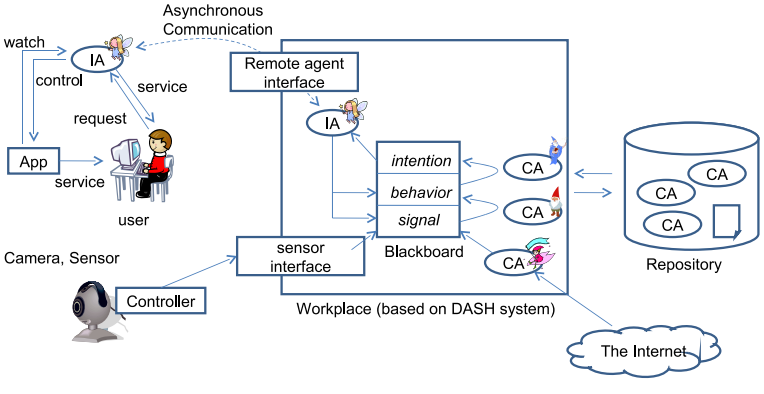


Fig. 2. Architecutre of B-DASH agent platform

3.2 Blackboard

The blackboard in the workplace is a storage for sensor data and assumption about human's behavior. Articles on the blackboard are shared by agents in the workplace.

The blackboard consists three layers. A signal layer is a layer which stores signal data from sensors. A behavior layer stores assumption of humans' behavior. Cognitive agents watch signals in the signal layer and infer humans' behavior.

Then cognitive agents write a result of the inference as an assumption on the behavior layer. An intention layer is a layer for writing humans' intention. Cognitive agents abstract from behavior to intention in the same way.

An example of an article on the blackboard is shown in Fig.3. An article is stored in the blackboard as Object-Attribute-Value triplet. Blackboard holds these articles with time stamp information.

```
(signal :place sensor-at-bookshelf
        :badge-id 9
        :time "2009-12-24 12:34:56")
```

Fig. 3. Article(Object-Attribute-Value triplet) stored in the blackboard

3.3 Cognitive Agent

Cognitive agent infers humans' behavior and intention using the blackboard. The blackboard is used by several cognitive agents.

An architecture of cognitive agent is shown in Fig.4(a). Cognitive agents are programmed using a rule-based programming language like DASH agent. Rules are processed by the rule engine. The Java object is used to do some complex procedures which cannot be described in the rule-based language, such as looking for resources from the internet.

A flow chart of the rule engine is shown in Fig.4(b). After initialization, cognitive agent starts watching the blackboard. When new article is written, the rule engine starts processing rules. If there are no more executable rules, the rule engine stops and waits until new article is written.

An example program for cognitive agent is shown in Fig.5. The program is written in the same way as DASH agent program. A rule "detect-movement" in the example is for detecting human's movement. It makes an assumption from two articles in the signal layer and writes the assumption on the behavior layer.

3.4 Interface Agents

As shown in Fig.1, Interface Agent works on the user PC. Interface Agent watches the applications working on the PC and controls them if necessary. It communicates with user to understand user's implicit/explicit request for DS. Then it provides information and services which is appropriate for the user.

In order to show agents' presence to the user, Interface Agent should work in user PCs, cell phones, information appliance devices, etc. But in this paper, we consider to develop Interface Agent which works only on use PCs like Microsoft office assistant. So the place where Interface Agent works is PC desktop, web browser, etc.

As shown in Fig.6, B-DASH system provides an asynchronous communication mechanism between user PC and Workplace PC. When an interface agent starts

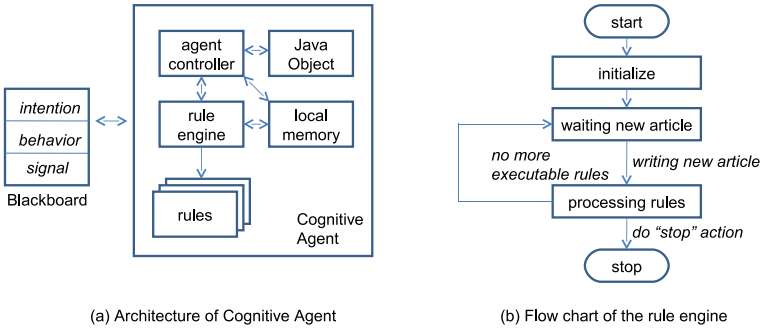


Fig. 4. Architecture of Cognitive Agent

```
(agent sample
    (rule detect-movement
        (signal :place ?place1 :badge-id ?id :time ?time1)
        (signal :place ?place2 :badge-id ?id :time ?time2)
       ~(signal :place ?p      :badge-id ?i  :time [> ?time1 < ?time2])
        -->
        (make (behavior :type movement :badge-id ?id
                        :from ?place1 :to ?plase2
                        :start ?time1 :end ?time2)) ))
```

Fig. 5. Example program for Cognitive Agent to detect Human's movement

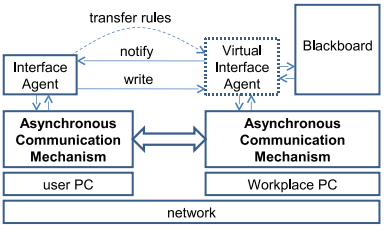


Fig. 6. Asynchronous Communication mechanism between Interface Agent and Blackboard

working on user PC, the mechanism transfers rules of the interface agent to the workplace and then Virtual Interface Agent starts watching the blackboard automatically. Using this mechanism, the interface agent can write articles on the blackboard on remote workplace PC. In addition, the virtual interface agent notifies changes of the blackboard to the interface agent. So it is easy to develop interface agents which uses the blackboard on remote PC because programmer does not have to concern complicated work about remote access.

4 Implementation

Now we are developing B-DASH system by improving DASH system. It has some useful user interfaces as shown in Fig.7.

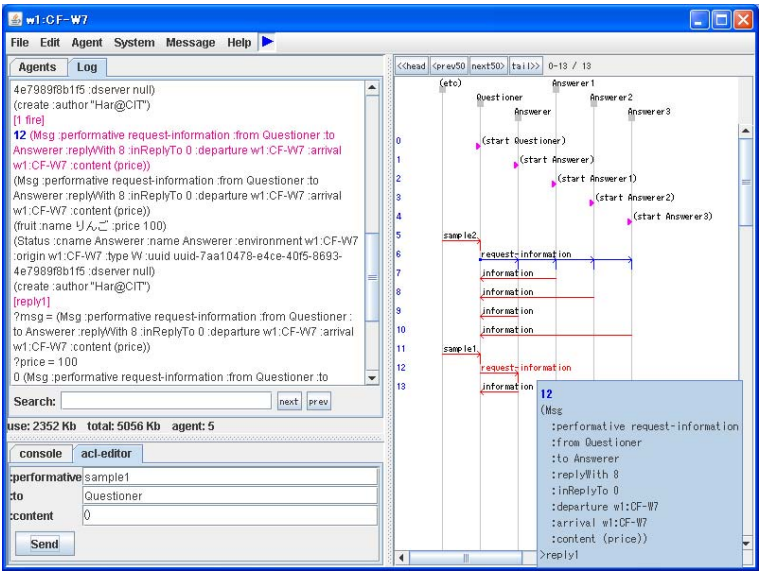


Fig. 7. GUI of B-DASH

B-DASH can receive data from the sensor described as follows.

Sensor at a door: It detects opening and closing of a door and writes this event with time on the blackboard.

Infrared receiver: For location detection, we use infrared equipments shown in Fig.8. In our laboratory, we wear the badge which sends an identification signal. When the infrared receivers detect the signal, they write ID signal and time on the blackboard.

Video camera: Motion of human and objects in the room was detected by using several cameras. Using a motion detection library [6], our platform can know brief information about motion of human and object in the room. The cognitive agents in the workplace use the information to make more precise information.

Sensor chair: It detects behavior of human who is sitting down on the chair. The chair is installed some sensors which detect rotation and acceleration of the chair. These sensors write motion event on the blackboard.

Using these sensors, we are now developing some applications. Fig.9 shows an example of application using B-DASH. This application visualizes behavior of human in our laboratory. Many sensors are installed in the room and they detect motion of human. Then it shows in this application.

Fig. 8. Infrared Receiver

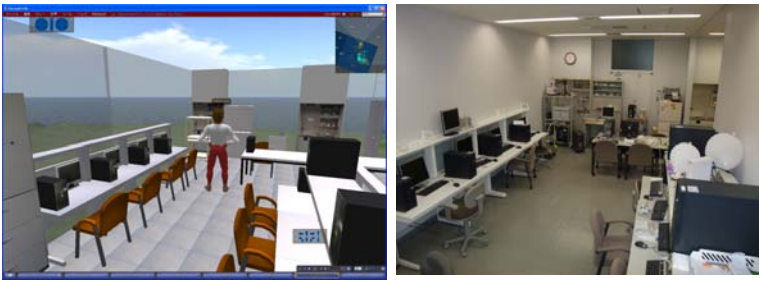


Fig. 9. Symbio Window

5 Conclusion

We described an agent-based platform called "B-DASH" for the Symbiotic Computing. Mutual cognition between human and agents is a key technology of the Symbiotic Computing. B-DASH can aggregate and share information using the blackboard mechanism to support developing software systems which can understand human behavior.

References

1. Uchiya, T., Maemura, T., Hara, H., Kinoshita, T.: Interactive Design Method of Agent System for Symbiotic Computing. International Journal of Cognitive Informatics and Natural Intelligence 3(1), 57–74 (2009)
2. Fujita, S., Hara, H., Sugawara, K., Kinoshita, T., Shiratori, N.: Agent-based design model of adaptive distributed system. Applied Intelligence 9(1), 57–70 (1998)
3. Sugawara, K., Maemura, T., Hara, H., Kinoshita, T.: A Concept of Symbiotic Computing and its Application to Telework. In: Proceedings of the 6th IEEE International Conference of Cognitive Informatics, pp. 302–311 (2007)

4. Sugawara, K., Fujita, S., Kinoshita, T., Shiratori, N.: A design of Cognitive Agents for Recognizing Real Space – Towards Symbiotic Computing. In: Proceedings of the 7th International Conference of Cognitive Informatics, pp. 277–285 (2008)
5. Hara, H., Sugawara, K., Kinoshita, T., Uchiya, T.: Flexible distributed agent system and its application. In: Proceedings of the 5th Joint Conference of Knowledge-based Software Engineering, pp. 72–77. IOS Press, Amsterdam (2002)
6. http://opencv.willowgarage.com/wiki/

An Extraction Method to Get a Municipality Event Information

Tatsuya Ushioda[1] and Shigeru Fujita[2]

[1] Graduate School of Information and Computer Science, Chiba Insutitute of Tchnology
[2] Dept.Computer Science, Chiba Insutitute of Tchnology, 2-17-1 Tsudanuma, Narashino, chiba, 275-0016, Japan
ushioda@sf.cs.it-chiba.ac.jp, Shigeru Fujita@it-chiba.ac.jp
http://www.sf.cs.it-chiba.ac.jp/

Abstract. It is an investigative purpose to acquire information on the event information page that exists in the municipality website in the form of a possible machine process. In this paper, we propose an extraction method from a HTML document based on dictionary.HTML tag is deleted from the HTML document and it converts it into the text. And, it proposes the method for extracting a target character string by comparing the text with the collection of words prepared beforehand. The evaluation experiment was done to the municipality in 23 Tokyo district and 56 Chiba prefecture in Japan. The proposal method was able to extract event information on as a whole 73%. The LR-Wrapper was 52%. The Tree-Wrapper was 55%. The PLR-Wrapper was 32%. The proposal method confirmed event information was rating higher than an existing method extractive by the combination of a simple algorithm and the collection of words.

Keywords: Text Mining, Web wrapper, Morphological Analysis.

1 Introduction

A municipality and a general enterprise use the website to do the giving information. There are event information and road works information as an example of information offered through each municipality website. These each municipality websites have aimed the use of the resident. Therefore, HTML is used for design to understand for the people, and not used to structure the document. Moreover, it is used by a usage different from the meaning of original HTML tag, and the information acquisition by mechanical processing is not considered.

It is thought that it is possible to reuse information that has already been acquired if the informaiton acquisition by mechanical processing becomes possible. For instance, it is possible to use it for a traffic guide in the vicinity of the place to which the event and construction are held. “A child’s watch support” can be done in using information excerpted from event information on the municipality. Moreover, because extraction information can be translated, municipality

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 128–137, 2010.

information translated besides Japanese can be offered. However, semantic web is not widespread under the present situation.

Up to now, to enable mechanical information acquisition, the information acquisition technique intended for the web page has been proposed. As for one, two or more web wrapper methods [2,3,4,5] for acquiring information from the HTML tag that is the feature of the web page are proposed. However, because how use the HTML tag is decided depending on the creator of the web page, it is necessary to generate wrapper of each web page. Therefore, a new cost is needed to generate wrapper whenever the design of each website is changed.

Moreover, the proper noun of the name etc. of the event and facilities tends to become various in event information though information acquisition method [6] by the degree of similarity of the character string is proposed. Therefore, when the degree of similarity is used, enough information acquisition cannot be done. Therefore, it is thought that the erroneous information is acquired.

In this paper, it proposes the technique for extracting event information that uses the word comparison from information open to the public on each municipality website. It experimented for the web page of 79 district, city and town.

2 Event Information

Information on the event of each municipality held in the region has been described on the event information page. And, more the design, the format of the web page, the number of cases of the content and information that has been described, the amounts of the explanation, and the qualities are various according to each municipality. Event information is extracted from the HTML document for the event information page. Not only the event name, the date and the place but also content of the event and various information on inquiries etc are described in event information. There is information that seems to be described on the event information page on each municipality website it. Information described by event information on the municipality website is shown as follows.

- Event name
- Date (The start date and the end date are included for the period).
- Place

Three kinds of above-mentioned information is enumerated. These information is extracted in this paper.

3 Related Work of Information Acquisition from Web

3.1 Category of Event Information Page

When the web page being offered by the municipality is treated, the form of the web page that should be considered is two forms [1].

– Single instance type[1]
  Web page in form from which only one event information is published in web page
– Multiple instance type[1]
  Web page in which two or more event information on the same category in web page is published.

These single instance type and multiple instance type are defined by Noguchi's research [1]. The unit of information that shows one such as the name, date, and Place of the event matter is called an instance in this.

3.2 Information Acquisition by Web Wrapper

The information acquisition method by web wrapper[2,3,4,5] looks for information by using the HTML tag that exists in the document. And, the text with the same meaning is a method assumed to be enclosed by the same HTML tag. In this method, the item to have to acquire the HTML tag and information beforehand is related. Finally, the related HTML tag acquires the described character string as a criteria.

There are a lot of researches on this method[2,3,4,5]. Therefore, various Wrappers have been developed. Those researches are described as follows.

LR wrapper[2]. The LR(Left-Right) wrapper requests a longest suffix and a longest prefix of information that should be acquired. It is a method for acquiring the text by using them. The probability of acquiring information other than target information lowers when the character string of the suffix and the prefix is long. However, such a character string might not be able to be decided mechanically.

Tree wrapper[3]. The tree wrapper treats the HTML document as a tree structure. And, it is thought that information with the same meaning as "Information that should be acquired" is enclosed by the HTML tag of the same tree structure. And, it is a method for acquiring the text enclosed by the HTML tag described by the corresponding tree structure.

PLR wrapper[4]. The PLR(Path-Left-Right) wrapper is a wrapper that combined the Tree wrapper with the LR wrapper. In the Tree wrapper, the text enclosed by the HTML tag specified from the tree structure of the HTML tag was acquired. Therefore, the unnecessary character string included in that was acquired together. It is a method for omitting an unnecessary character string that depends on taking the concept of LR wrapper to this and exists.

Use of two or more Web wrapper[5]. To correspond to two or more web pages, the correct answer data is studied from a part of information that should be acquired. And, the method for combining the LR wrapper composed by two or more patterns combining it is proposed[5].

3.3 Problem of Related Work [2,3,4,5]

A common problem to these methods is things that use and the structure of the HTML tag change because the design of the web page changes. Therefore, there is a possibility that the meaning is different even if the same HTML tag is used. Therefore, whenever the design of the web wrapper is changed, it is necessary to generate the wrapper. These wrapper method extract information by using the HTML tag. Therefore, tag is extracted when two or more different information is described while having been enclosed with one HTML tag and targeted information alone cannot be extracted only by using it.

3.4 Information Acquisition by Degree of Similarity of Character String[6]

There is Umehara's "Semiautomatic conversion from series type HTML document based on the case" as a technique for paying attention to the character string. It differs from the method that uses the web wrapper, the HTML tag doesn't possess great significance, and it uses it to assume the delimitation of the text that appears in the document. This document is called series type HTML document. It corresponds to the document to which the meaning of the document structure and information is mutually similar. It is the one to acquire information by using the case document. It is the one to acquire information from the document of the same series in giving the document that becomes a case. Therefore, it is a method expected that effective information acquisition can be done when the web page that offers regional information is a series type document. There is a possibility to be able to correspond even when the design of the web page is changed because it acquires it from the viewpoint of degree of similarity of the character string unlike the web wrapper method. Therefore, the wrapper of each web page need not be generated.

However, a peculiar proper noun of the name etc. of the event and facilities tends to become various in event information. Therefore, enough information acquisition cannot be done to the degree of similarity of the character string and there is a possibility of acquiring the erroneous information.

4 An Extraction Method for a Municipality Web Site

To aim with this paper is to extract event information on the event information page that exists in each municipality. The event name, the date, the place, and the extra information have been described in this event information.

Figure 1 shows the flow of the proposal method. The proposal method extracts information by using the collection of words from the HTML document where event information is described. The proposal technique doesn't extract information by using tag. Therefore, it is thought that the information extraction is possible even by the web page that cannot be extracted by the association study. It is necessary to use the collection of words that collected words concerning event information to use the proposal method. The collection of words is

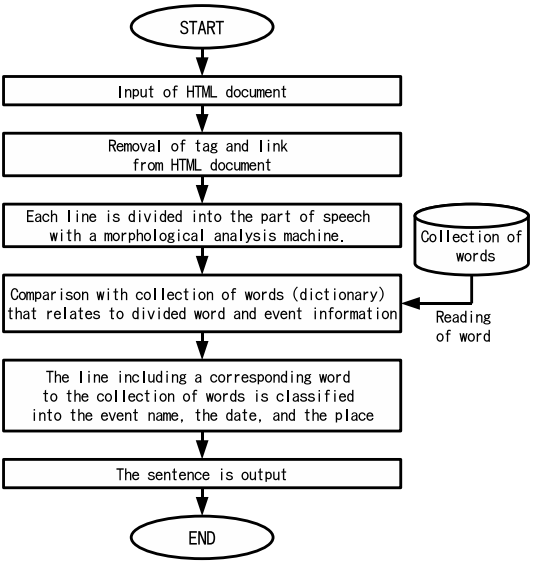


Fig. 1. Event information extraction method

event name, date, place, and exclusion. The word concerning information not to be extracted this time is collected as "exclusion". Moreover, the morphological analysis machine used by this processing is "Sen" [7].

Next, the collection of words used this time is described. Each collection of words acquires each municipality event information page beforehand as the training example. The word with high occurrence rate is collected and registered in sentences where the event name, the date, and the place are described on the event information page. The collection of words of exclusion collects and registers the word with high occurrence rate in sentences similarly excluded.

The content of each collection of words, the example of the word, and the number of words are described as follows.

1. Collection of words (event name)
   Collection of words that collects words concerning event name (80 words in total)
   – Example of word

   大会 (a general meeting)　　講座 (a chair)　　マーケット (a market)

2. Collection of words (date)
   Collection of words that collects words concerning date (18 words in total)
   – Example of word

   期日 (a date)　　正午 (noon)　　開場 (opening)

3. Collection of words (place)
   Collection of words that collects words concerning place (46 words in total)
   – Example of word

   会場 (the grounds)　　図書館 (a library)　　会館 (a hall)

4. Collection of words (exclusion)
   Collection of words concerning "Sentences not extracted" that collects words (15 words in total)
   – Example of word

   参加 (join)　　問い合わせ (an inquiry)　　申し込み (a reservation)

Sets of these words register only the word that relates to event information. Event information from the text is described in the next paragraph.

Preprocessing. The HTML tag and the hyperlink are removed from the HTML document as a preprocessing of the event information extraction. This processing makes the HTML document only text information. It is suppressed that a needless information extraction is done by the result and the following processing. Moreover, there is a link to another event information page in the event information page. Each event name is described in it without fail.

Information extraction by word comparison. The HTML tag and the hyperlink are removed from the HTML document by the preprocessing and it makes it to text information.

This method extracts target information based on the word of the collection of words reading each sentence described in event information. Next, the line read by using Japanese morphological analysis machine Sen is divided into the part of speech. It compares it by using the collection of words. The reason to use the morphological analysis machine is that there is no blank between parts of speech of a Japanese sentence. Therefore, it is necessary to divide into the part of speech once. The line that matches to the word of the collection of words is classified into the event name, the date, the place, and exclusion according to the kind of the collection of words. The word is registered in the collection of words of the event name, the date, the place, and exclusion respectively. The line classified into the event name, the date, and the place is output as it is. At this time, when it is more than the number of parts of speech of the longest sentences in the sentence from which the number of parts of speech of lines is classified into the event name, the date, and the place, it doesn't output it. The purpose of this is not to output those sentences when the long sentence of the explanation etc. is included in the classified sentence.

It is thought by the sentence including the matched word that the possibility that the content concerning the word is described is high. Therefore, it is thought that target information can be extracted. However, the sentence classified into exclusion is not output. Information that doesn't depend on the HTML tag described in event information is extracted by this method.

5 Experiment

5.1 Data for Experimental Environment and Evaluation

The experimental evaluation system was made with JDK1.6, and it experimented by the experimental environment in Table 1. The page treated by the assessment experiment is total 230 page to which event information on 23 Tokyo district on January 10, 2009 and event information on Chiba 35 prefecture city and town were described. The municipality where event information doesn't exist is not targeted this time.

Table 1. System for evaluation

Programing Language	JDK 1.6
HTML Parser	Jericho HTML Parser
Morphological analysis machine	Sen Version 1.2.2.1
Registered number of words	159 words in total

Each municipality is collecting the event information pages by five pages. However, these are the numbers of pages to which event information is described. Therefore, the number of pages is not necessarily the same as the number of event information.

5.2 Evaluation Approach

The event information pages collected in the system that mounts the proposal method are given. The extraction result of an individual web page is evaluated by using "Accuracy" explains by the following clause. Moreover, the side-by-side test on the association study was done by using the same data.

5.3 Evaluation Figure

Event information actually described information acquired by using the proposal method on the web page is compared. It evaluates how many the number of information correctly acquired is.

The definition of accuracy (Accuracy) (%) shown in expression (1) as a standard of the evaluation is used.

$$Accuracy = \frac{\sum_{j=1}^{n} C(Eventname_j, date_j, Place_j, Others_j)}{(Total\_of\_event\_information \times 4) - X} \times 100 \qquad (1)$$

X:Total where information that in each event information should doesn't exist

$$However, C = \begin{cases} The\_event\_name\_exists + 1 \\ The\_date\_exists + 1 \\ The\_place\_exists + 1 \\ Others\_exist + 0 \\ Others\_don't\_exist + 1 \end{cases}$$

In the targeted web page, two or more instances exist. Therefore, C that exists in the molecule of expression (1) is extracted information total of one (Others) to be excluded of each event information besides event name (Eventname), date (date), and place (Place). To extract information from the text in the proper move method, needless information is extracted. Moreover, needless information is treated as one set. Needless information is information that should not be extracted. Therefore, only when each instance is not extracted, one is added to the total of C as well as other information. Moreover, Total_of_event_information is total of all event information. X is a number that doesn't exist in information that each event information should acquire. The total of the denominator is total of all information in the web page where input event information is described. The proposal method evaluated how much the number of information that was able to be extracted compared with former number of information was.

5.4 Outcome of an Experiment

When the web page where event information is described is assumed to be an input, the event information extraction result is shown in Table 2.

The value of the accuracy of 23 Tokyo district, 31 Chiba prefecture city, and 4 Chiba prefecture town is indicated in Table 2. The accuracy is a value in which expression (1) defined in the preceding clause is used and calculated. The number of all information is the values of the denominator of expression (1), and the total of all information that exists on the web page is shown. As for the acquisition information total, it is a value of the molecule of expression (1). It is information total extracted by comparing the extraction result by the assessment experiment with former HTML document. Moreover, it experimented by using data as which the association study was the same. The result is similarly shown.

5.5 Consideration

The result of using the PLR wrapper method in Table 2 generates "Pass" to extract a target character string by the frequency of the character string that appears in the page as a low reason. This PLR wrapper method gives the training example as well as the LR wrapper method and the Tree wrapper method. However, information at which position on a target character string besides the training example exists is not given. It is thought that event information cannot be extracted for that.

The outcome of an experiment whether needless information was extracted is compared in the experiment with former HTML document and it does. As for the proposal method, needless information more than the relation research is not extracted. The event information page uses the headword for this. Therefore, because the word that shows information such as "Inquiry" and "Application" not extracted was corresponding to the word of the collection of words, it has not been extracted.

When the place of the event is described after "Inquiry" and "Application" again, the problem of the proposal method is extracted. The page to which the

address in the place was extracted two times while experimenting existed in 40 % of data for the evaluation. There is one method of preventing such a thing from happening. About not comparing words concerning the place, it is a method after that when the line concerning the place is extracted once. However, it is not possible to correspond to the multiple instance type by this method.

Moreover, the proposal method is a method that doesn't use the HTML tag. Whenever the design of the page is changed like the Web wrapper method, a new Wrapper is not generated for that. However, the word registered in the collection of words to use the word for the comparison becomes important. When peculiar word to various places might be used for the event name and the place, and the word is not registered, it is not likely to be able to extract it. This is thought to be an occurrence of a similar problem when doing to the event information page of other each municipality that doesn't do the assessment experiment this time. This problem solving method prepares the collection of words that collects the word that the occurrence rate is high the event name, the date, and each place. There is a method of using the collection of words that collects words that become features in each municipality with an existing collection of words. In this case, the necessity for registering a new word in the collection of words is caused. However, it is thought that it is possible to correspond to a new event information page by registering a peculiar word to the region.

It experimented for each municipality event information page this time. The targeted page is page to which event information has been described, and it doesn't experiment in the state without prior knowledge. However, this event information page group is often collected to one place in each municipality website. Therefore, it is thought that only the event information page can be acquired if the place where those pages exist is understood.

6 Conclusion

There is a lot of useful information in the web page that the municipality has opened to the public. However, the information extraction by the machine process is difficult because it has aimed at what the resident sees.

An existing web wrapper method [2,3,4,5] solves this problem by extracting information by using the HTML tag. However, there was a problem that target information was not able to be extracted in these methods when information that had to be extracted was not enclosed directly by the HTML tag.

To extract event information that was not able to be applied to this problem by an existing method with this paper, it proposed the extraction method that used the word comparison from text information that removed the HTML tag from the HTML document.

An existing method and the side-by-side test were done by using the municipality event information page of 23 Tokyo district and 35 Chiba prefecture city and town to confirm the effectiveness of the proposal method. But, the municipality where event information doesn't exist is excluding from the evaluation. The accuracy of expression (1) was used as evaluation figure. As for the

outcome of an experiment, event information on 73% was able to be extracted to the proposal method. Moreover, the LR wrapper method is 52%. The Tree wrapper method is 55%. The PLR wrapper method was able to extract event information on 32%.

The proposal method is an algorithm that is simpler than the algorithm of an existing method. Moreover, it was confirmed to be able to extract event information by having used the collection of words made beforehand.

References

1. Noguchi, R., Yamada, Y., Ikeda, D.: Template Rxtraction from Web Documents using Substring Amplification. In: DEWS (2004)
2. Kushmerick, N.: Wrapper induction: Efficiency and Expressiveness. Artificial Intelligence 118(1-2), 15–68 (2000)
3. Yshitsugu, M., Hiroshi, S., Hiroki, A., Arikawa, S.: Extracting Text Data from HTML Documents. Information Processing Society of Japan 42(14), 39–49 (2001)
4. Yamada, Y., Ikeda, D., Sachio, H.: Automatic Tree and String Based Wrapper Generation for semi-structured Documents. IPSJ SIG Notes 2003 98, 115–122 (2003)
5. Yukio, U., Toshio, U., Ryoji, K., Tohgoro, M., Ohwada, H.: Information Extraction Using Specic Rule Wrapper Array. IPSJ SIG Notes, 117–123 (2007)
6. Masayuki, U., Koji, I., Hirokazu, N.: A Case-Based Semi-automatic Transformation from HTML Documents to XML Ones - Using the Similarity between HTML Documents Constituting a Series. Journal of Japanese Society for Artificial intelligence 16(5), 408–416 (2001)
7. Sen home, https://sen.dev.java.net/

Design and Implementation of Adaptive Inter-platform Communication Mechanism for Agent-Based Framework in Ubiquitous Computing Environment

Taishi Ito[1,2], Hideyuki Takahashi[2], Takuo Suganuma[1,2], Tetsuo Kinoshita[1,3], and Norio Shiratori[1,2]

[1] Research Institute of Electrical Communication, Tohoku University, 2-1-1, Katahira, Aoba-ku, Sendai, Japan
[2] Graduate School of Information Sciences, Tohoku University, Aramaki Aza Aoba 6-3-09, Aoba-ku, Sendai, Japan
[3] Cyberscience Center, Tohoku University Aramaki Aza Aoba 6-3, Aoba-ku, Sendai, Japan

Abstract. Recently, various computing technologies such as embedded computer, and wireless access networks etc. are in general use, and applications in ubiquitous computing (ubicomp) environments are widely spread. In this paper, we propose an advanced flexible communication infrastructure for agent-based middlewares in ubiquitous computing environments. We focus on an communication scheme between agent platforms, which can flexibly select a appropriate communication scheme based on properties of inter-agent communications and computational resource statuses. We performed some experiments by using a prototype system and confirmed our proposed communication scheme works effectively.

Keywords: Ubiquitous Computing, Agent, Framework, Mobile Computing, Adaptive Communication.

1 Introduction

Recently, advanced computing technologies such as embedded computer, mobile terminals, sensor networks, and wireless networks are commonly used, and ubiquitous computing (ubicomp) environment based on these technologies is becoming a part of people's lives. In general, however, limitations of availability of computer and network resources exist, thus application systems that work on the ubicomp environment, that is called ubiquitous applications, are required to have ability of adaptation to various types of the environments. They also have to cope with decentralization of contexts and services [1,2]. Hence the middleware to develop the ubiquitous applications more effectively is promising [3]. Meanwhile, studies on agent-based middleware are investigated recent years. Because multiagent system built on the agent-based middleware has high adaptation ability to environments.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 138–151, 2010.

Table 1. Inter-platform communication schemes of typical agent-based middleware[4]

Agent-based middleware	Developer	Used communication schemes
Ajanta[5]	University of Minnesota	Java RMI, ATP
FIPA-OS[6]	Open Source	ACL, IIOP, RMI
Grasshopper[7]	IKV++ Technologies AG	sockets, RMI, IIOP
JADE[8]	TILab	ACL, RMI
Zeus[9]	British Telecom. Lab	KQML, ACL
DASH[10]	Chiba Inst. of Tech.	ACL, RMI

Therefore, it is expected to be a potential framework to develop the ubiquitous applications effectively. Our study aims to provide advanced and stable services in ubicomp environment by using agent-based middleware. In this paper, we focus on the problem concerning the instability and inefficiency of communication between agents. We propose an "Adaptive Inter-platform Communication Mechanism" that can flexibly change the inter-platform communication schemes according to the situations of network or computational resources and properties of inter-agent communications. This mechanism enables the agent platform to adapt to the various kinds of inter-agent communication requirements. In this paper, we present details of the design of the Adaptive Inter-platform Communication Mechanism. In addition, we performed some experiments in order to confirm the effectiveness of the proposed scheme.

2 Related Work and Problems

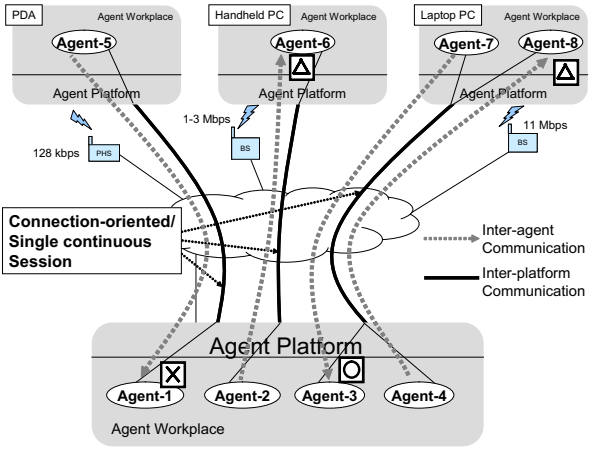
2.1 Ubiquitous Application Based on Agent-Based Middleware

From the system development viewpoint, there is an existing study that has investigated a middleware specialized in developing ubiquitous applications [3]. The paper describes as the functional requirements to the middleware (R1) Adaptability to changing environment, (R2) Flexibility to compose application dynamically, and (R3) Cooperativeness to share information between various. On the other hand, researches and developments of variety of agent-based middleware have been promoting in recent years [5,6,7,8,9,10,11,12]. The agent-based middleware is a software infrastructure to construct multiagent system. The multiagent system has a characteristic to adapt to the various situations by changing the combination of agents. Therefore, the system can be constructed flexibly according to the situations. From these reasons, the multiagent system can fulfill the functional requirements (R1) to (R3), and it would be suitable to construct ubiquitous applications as the multiagent system.

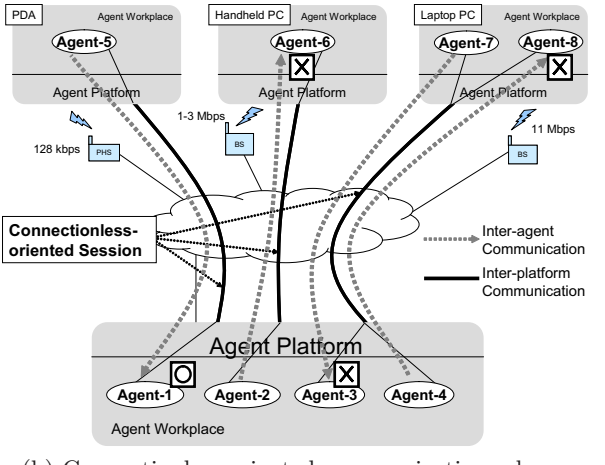
2.2 Difficulties

We have some difficulties when the agent-based middleware is applied to the ubicomp environment. First, **(P1) Instability and inefficiency of**

communication among entities is mainly caused by the restriction on the resources of the wireless networks. Second, **(P2) Performance degradation** is due to the limitation of the computational resources and the excessive load of agents on small size devices. Third, **(P3) Low scalability** is a problem of low extensibility in terms of the function and size of the overall system. This originates from (P1) and (P2). Last, **(P4) Complexity in deployment** is an operational issue in practical use; how to deploy the agent platform on the heterogeneous computing environments.



(a) Connection-oriented, single continuous session communication scheme



(b) Connectionless-oriented communication scheme

Fig. 1. Issues in inter-platform communication by using single communication scheme

Table 2. Examples of inter-agent communication semantics

Type	Sender	Recipient	Communication semantics
(A)	Agent-5	Agent-1	Periodical and continuous report of user's physical location
(B)	Agent-2	Agent-6	Agent termination request
(C)	Agent-7	Agent-3	Transfer of operational history after the service completes
(D)	Agent-4	Agent-8	Transmission of contract net protocol message

2.3 Target Problem

In this paper, we focus on the problem (P1). In ubicomp environment, because the network with narrow bandwidth and unstable connection are generally used, the improvement in efficiency and stability of the communication between agent platforms (inter-platform communication) is essential. However, existing agent-based middleware has limitations to resolve this problem. This is because, one and only one communication scheme is statically used in the inter-platform communication even if the types of the communication environments are different. We show the typical agent-based middleware and those inter-platform communication schemes in Table 1. In Table 2, we show some examples of semantics of inter-agent communication. Suppose that these different types of communications between agents are performed over the single communication scheme between agent platforms. We show the specific examples in Fig. 1 to clarify this problem. In Fig. 1(a), the agent-based middleware with this communication scheme has an advantage when reliable communication between agents is required, and the wide bandwidth of network can be available. However, for the inter-agent communication which needs real-time transfer such as delivering of user's location information, and if the network connection is unstable, then the requirement cannot be fulfilled due to the transmission delay. In this case, the communication type (C) in Table 2 is suitable, but (A) is not suitable. On the other hand, Fig. 1(b) depicts the inter-platform communication scheme by using a connectionless-oriented transport service. In this case, it has an advantage when the inter-agent communication requires real-time transmission rather than the reliability. By contrast, when the reliability is needed such as the case of agent termination instruction is issued, some problems may occur in cooperative behavior of agents due to no arrival of the important message. In this case, (A) is suitable, but other types are not suitable. These examples show that, existing inter-platform communication with a single communication scheme cannot achieve the improvement in efficiency and stability of the inter-agent communication in ubicomp environment where the absolute amount of network resources and computer resources are restricted and the change of them are drastic.

3 Adaptive Inter-platform Communication Mechanism

3.1 Outline of the Proposed Mechanism

To resolve the problem described in Section 2.3, a mechanism is required to switch many types of inter-platform communication schemes according to the

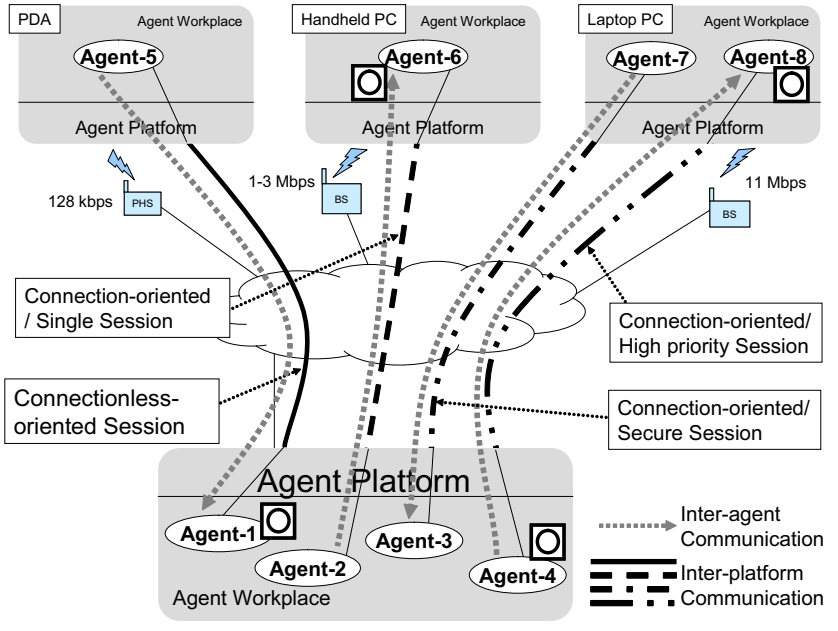


Fig. 2. Examples of the appropriate selection of the inter-platform communication scheme based on the inter-agent communication semantics

information of environment in which the agent-based middleware works, and the properties of the inter-agent communications.

Fig. 2 shows the effect of the proposed mechanism. The assumed inter-agent communication semantics are the same as those defined in Table 2. This mechanism selects the communication scheme of low transmission delay when the inter-agent communication requires real-time property. Whereas it offers the communication scheme with reliability when the agent needs the reliable communication instead of the real-time property. Therefore, the agent platform can be achieved, with the flexible inter-platform communication which meets the requirements of the inter-agent communications as much as possible.

We propose an "Adaptive Inter-platform Communication Mechanism." This mechanism has functions to select a suitable inter-agent platform communication scheme based on the situations of network and computational resources and the properties of inter-agent communications. The inter-platform communication scheme M is represented by the five tuples as follows:

$$M =< c, a, b, p, s >$$

Here, c represents a connection type of the transport communication such as connectionless-oriented or connection-oriented; a shows a kind of the transport session such as single or continuous session; b expresses a kind of data transmission scheme such as streaming or bulk data transfer; p means a priority of an

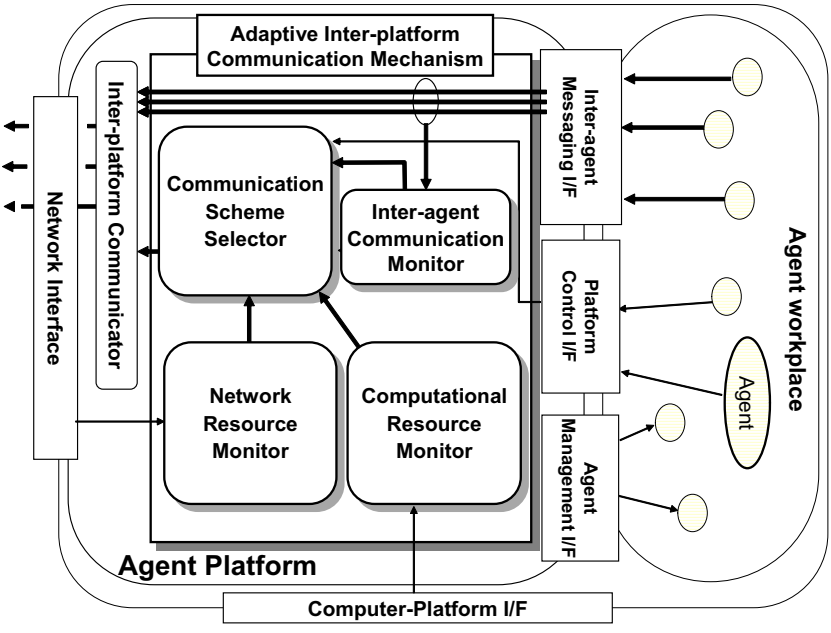


Fig. 3. Architecture of Adaptive Inter-platform Communication Mechanism

agent message such as high, medium, low, and urgent; and s is a security property such as encrypted or plain. The proposed mechanism outputs the selected communication scheme in the form of this model.

3.2 Architectural Design of the Proposed Mechanism

Fig. 3 shows the architectural design of Adaptive Inter-platform Communication Mechanism. This architecture consists of six functions. The **Computational Resource Monitor** function observes the computational resources of the computer, such as CPU usage rate and memory consumption status. The **Network Resource Monitor** function manages the network-related data obtained from network interface, such as the type of communication link, and available or utilizing network bandwidth. The **Inter-agent Communication Monitor** function observes inter-agent communications, and it infers the charasteristics of the inter-agent communication. The **Communication Scheme Selector** function is a key component. It makes a decision about suitable inter-platform communication scheme M based on the monitoring functions. The **Inter-platform Communicator** function selects a communication scheme that satisfies the suggestion. The **Network Interface** function establishes and maintains a link of the inter-platform communication and transfers agent messages through the link. It also gives information about network resource situations.

3.3 Internal Structure of Communication Scheme Selector

Information that is given to the Communication Scheme Selector from various monitoring functions is diverse. If the function for decision making on appropriate communication scheme is written by the procedural type programming language, there will be problems in its description and readability. In this work, we propose the design of this function with the "production system" to resolve these problems. The employment of the production system enables the stepwise refinement of the function.

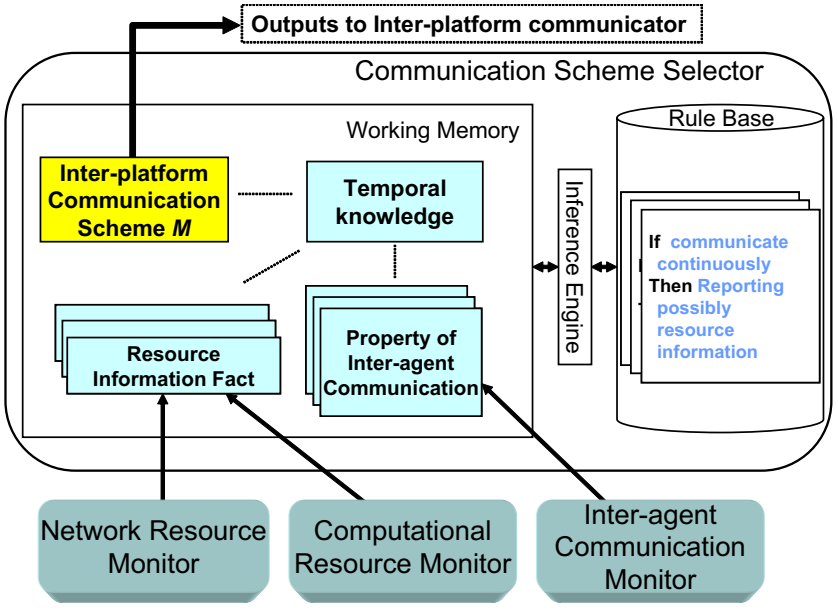


Fig. 4. Internal structure of Communication Scheme Selector based on production system

The internal structure of this function is shown in Fig. 4. The Working Memory(WM) stores a set of Facts that represents a situation obtained from various monitoring functions. The Rule Base stores a set of rules that represents a production rule for constructing intermediate knowledges. The intermediate knowledge is used in the process of inference, the final inference result, etc. Finally the rule derives a appropriate communication scheme M.

The rule that generates the intermediate knowledge not use all facts in WM but only uses several and partial facts. For this reason the intermediate knowledge is also partial and temporary and these intermediate knowledge can compete each other. For treating the competitive situation, we included "Positive Suggestions of M" and "Negative Suggestions of M" to the intermediate knowledge and output M by aggregating these options. In doing so, ubiquitous application programmer can make the rule without considering other rules.

3.4 Example of Operation of Communication Scheme Selector

Here, facts are generally represented in the following form.

$$(identifier \ : attribute \, [value] \, ...) \tag{1}$$

And structure of intermediate knowledge are generally represented in the following form.

$$\begin{array}{l}(inference - result \\ \quad : communication \, [communication \, endpoint] \\ \quad : positive \, [positive \, suggestion \, of \, M] \\ \quad : negative \, [negative \, suggestion \, of \, M] \\ )\end{array} \tag{2}$$

The *:communication* attribute indicates a communication endpoint of inter-agent communication, and the *:positive* attribute is a positive suggestion and the *:negative* attribute is a negative suggestion.

Next we describe an example of operation of the Communication Scheme Selector. First, the Network Resource Monitor function observes a situation: "The Round Trip Time(RTT) between this machine and a remote machine X is 2,500 millisecond.", and the Inter-agent Communication Monitor function observes a situation: "Agent A is communicating with Agent B in a remote machine X at interval of 10,000 millisecond.". Hereby, the following facts are becoming in WM.

$$\begin{array}{l}(ping\text{-}update \\ \quad : remote\text{-}address \, X \ : rtt\text{-}millisec \, 2500 \\ )\end{array} \tag{3}$$

$$\begin{array}{l}(agent\text{-}outgoing\text{-}communication \\ \quad : from \, A \ : to \, B \\ \quad : remote\text{-}address \, X \ : remote\text{-}platform \, P \\ \quad : frequency\text{-}millisec \, 10000 \\ )\end{array} \tag{4}$$

Next, for example, a threshold value of the RTT is set to 2,000 millisecond. and a threshold value of transmission of inter-agent communication interval is set to 10,000 millisecond. The first threshold value is used for determining whether a situation of network is overflow or not, and the next threshold value is used for determining whether a situation of inter-agent communication is high-frequency or not. Hereby, the following facts are becoming in WM.

$$(rtt\text{-}threshold \ : threshold \, 2000) \tag{5}$$

$$(frequency\text{-}threshold \ : threshold \, 1000) \tag{6}$$

Consequently, from Fact (3) and Fact (5), the production engine infers the following intermediate knowledge. This knowledge means that it is feasible to use no reliable communication scheme and not to use reliable communication scheme.

```
(inference-result
  : communication
    (link : from * : to * : remote-address X : remote-platform *)
  : positive
    (suggestion : guarantee-type (NoReliable) ...)
  : negative
    (suggestion : guarantee-type (ReliableArriveOne) ...)
)
```
(7)

In the same way, the production engine infers the following intermediate knowledge from Fact (4) and Fact (6). This knowledge means that it is feasible to use reliable communication scheme.

```
(inference-result
  : communication
    (link : from A : to B : remote-address X : remote-platform P)
  : positive
    (suggestion
      : guarantee-type (ReliableArriveOne) ...)
  : negative
    (suggestion
      : guarantee-type () ...)
)
```
(8)

In addition, the Network Resource Monitor function observes a situation; Reliable communication scheme and No reliable communication scheme is available. The production engine infers the following intermediate knowledge.

```
(inference-result
  : communication
    (link : from * : to * : remote-address * : remote-platform *)
  : positive
    (suggestion
      : guarantee-type (ReliableArriveOne NoReliable) ...)
  : negative
    (suggestion
      : guarantee-type (ReliableArriveSome) ...)
)
```
(9)

The *:communication* attributes of Fact (7), Fact (8), and Fact (9) are corresponding to the communication of Agent A and Agent B. Therefore, the Communication Scheme Selector summarizes these facts to the following fact.

```
(suggestion-set
  : communication
    (link
      : from A : to B
      : remote-address X : remote-platform P)
```

$$
\begin{array}{l}
\quad : positive \\
\quad\quad (suggestion \\
\quad\quad\quad : guarantee\text{-}type \\
\quad\quad\quad\quad (NoReliable\ ReliableArriveOne)\ ...) \\
\quad : negative \\
\quad\quad (suggestion \\
\quad\quad\quad : guarantee\text{-}type \\
\quad\quad\quad\quad (ReliableArriveOne\ ReliableArriveSome)\ ...) \\
)
\end{array}
\tag{10}
$$

Fact (10) shows an inference result from intermediate knowledge. This result denotes when Agent A communicates with Agent B in platform P in machine X, *NoReliable* or *ReliableArriveOne* is feasible to communication scheme, but *ReliableArriveOne* and *ReliableArriveSome* are not feasible. Finally, the production engine subtracts *:negative* from *:positive* of Fact (10), and the following fact led as a final inference result M.

$$
\begin{array}{l}
(M\ : communication \\
\quad : (link\ : from\ A\ : to\ B\ : remote\text{-}address\ X\ : remote\text{-}platform\ P) \\
\quad : guarantee\text{-}type \\
\quad\ NoReliable \\
\quad ...)
\end{array}
\tag{11}
$$

Fact (11) draws an inference result. This means to use not reliable communication scheme when Agent A communicates with Agent B in platform P in machine X.

4 Experiment and Evaluation

4.1 Experimental Environment and Scenario

We performed an experiment to confirm the effectiveness of proposed mechanism by using the prototype system. To confirm the advantage of the proposed mechanism, we performed a similar experiment with an agent system which can use single inter-platform communication scheme (TCP) in the same network situation. The experimental environment consists of two PCs as shown in Fig. 5. We assume the environment where a server transmits the real-time data streaming to a receiving terminal. The receiving terminal is supposed to be a handheld PC and it is connected with the low bandwidth and unstable wireless access network such as PHS. The PHS is an best-effort network service and that of up-link bandwidth is 68 kbps and down-link bandwidth is 128 kbps. We installed a "Server" agent on the server and a "Controller" agent on the receiving terminal. On the receiving terminal side the Controller agent observes the network situation, and sends the request of control of the data transmission rate to the Server agent if necessary. The Server agent receives this request, and controls the data transmission rate.

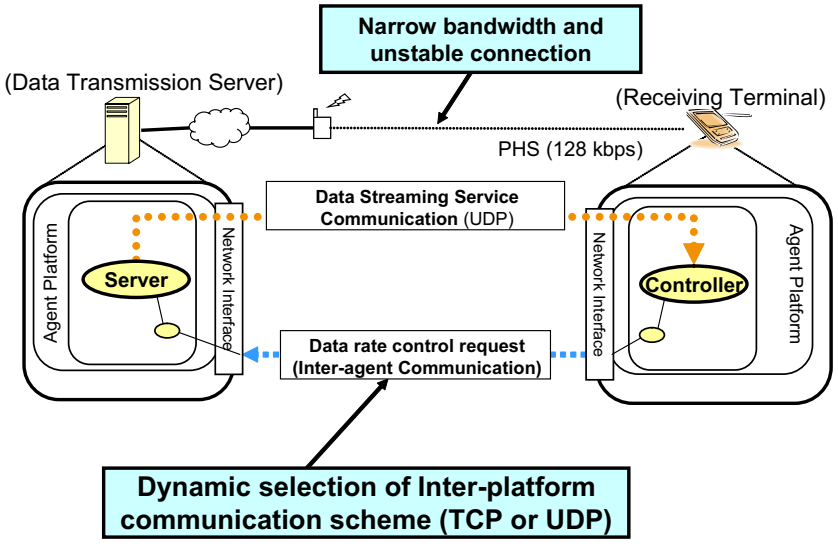


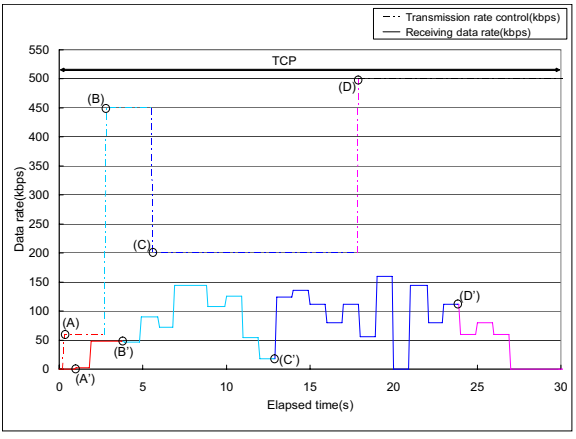
Fig. 5. Experimental environment

Here, the Controller agent sends a sequence of transmission rate control messages in order of 60 kbps, 450 kbps, 200 kbps, 500 kbps, 10 kbps, 20 kbps in every 2.5 s to the Server agent.

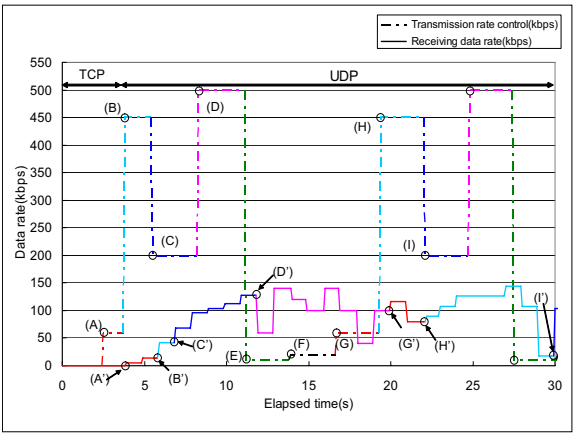
4.2 Experimental Results

The result when the communication scheme is fixed to the connection-oriented communication is shown in Fig. 6(a), and the result of the prototype system by using the Adaptive Inter-platform Communication Mechanism is shown in Fig. 6(b). The horizontal axis represents elapsed time, and the vertical axis is data rate (kbps). The broken line drawn in this graph means the transmission data rate control, and a solid line means the received data rate. Circles on the solid line show the time when the received data rate is actually changed to the value specified by transmission data rate control just before. For instance, the change of received data rate at point (A') is caused by the transmission data rate control at point (A), and also change at (B') is caused by (B), and at (C') is caused by (C), respectively. We call this duration "Response Time". Moreover, the "TCP" and "UDP" in Fig. 6(a) and (b) means the communication scheme used at the time. In (a), the result shows that the network situation was unstable from 5 s to 30 s. This is because the specified value of transmission rate control was exceed the available bandwidth greatly in both cases. However, the time length when user-level QoS was unstable was shortened in (b).

Here we compare the results from the viewpoint of Response Time. The average Response Time was 4.03 s in (a) and 4.23 s in (b). In (a), The Response Time at (C)-(C') was 7.4 s and at (D)-(D') was 6.1 s; those was very longer



(a) A result by the fixed communication scheme of connection-oriented communication (TCP)



(b) A result by the prototype system

Fig. 6. Experimental results

than an average Response Time. This is because the transmission rate control request was transferred with TCP in the bad network condition, and so transmission control in transport layer such as congestion control or retransmission worked. Thus, significant delay of the request message occurred. By contrast, in (b) the transmission rate control request was transferred with UDP at (E) and (F) in the bad network condition. Here, the UDP datagram which contains the rate control request was lost and the request was ignored. In the graph of (b), we can find this phenomenon by disappearance of (E') and (F'). However, the uncontrollable situation was recovered faster that the case of (a), because (G)

was affected in (G') rapidly and the stable situation continued after 20 s. This means that the time length when user-level QoS was unstable was shortened by the appropriate selection of the communication scheme.

4.3 Discussion

The experimental result indicates that data were transmitted accurately by the UDP as a communication scheme when the network resources are degraded. Because of the time cost for switching communication scheme is less than 1 ms, we think the prototype system is suitable for the practical use.

From these experimental results and evaluation, we finally confirmed that the agent-based middleware can provide stable and high-quality services by switching adaptively the inter-platform communication scheme according to the situation of environment.

5 Conclusion

In this paper, we proposed an adaptive communication mechanism between agent platforms which can flexibly select communication schemes based on the properties of inter-agent communication, to achieve stable ubiquitous services by using agent-based middleware. We described the design of the outline of the Adaptive Inter-platform Communication Mechanism. In addition, we performed an experiment using the prototype system. We confirmed that the proposed mechanism can maintain quality of ubiquitous services. In future work, we will continuously enhance the functions of the prototype system, such as the Inter-agent Communication Monitor, Communication Scheme Selector, and inference engine of the internal processing.

References

1. Soldatos, J., Pandis, I., Stamatis, K., Polymenakos, L., Crowley, J.L.: Agent based middleware infrastructure for autonomous context-aware ubiquitous computing services. Computer Communications 30(3), 577–591 (2007), Special Issue: Emerging Middleware for Next Generation Networks
2. Broens, T., Quartel, D.A.C., van Sinderen, M.: Towards a context binding transparency. In: Pras, A., van Sinderen, M. (eds.) EUNICE 2007. LNCS, vol. 4606, pp. 9–16. Springer, Heidelberg (2007)
3. Grimm, R., Davis, J., Lemar, E., Macbeth, A., Swanson, S., Anderson, T., Bershad, B., Borriello, G., Gribble, S., Wetherall, D.: System support for pervasive applications. ACM Trans. Comput. Syst. 22(4), 421–486 (2004)
4. Nguyen, T.G., Dang, T.T.: Agent platform evaluation and comparison. Technical Report Pellucid 5FP IST-200134519, Institute of Informatics, Slovak Academy of Sciences (June 2002)
5. Ajanta, http://www.cs.umn.edu/Ajanta/
6. FIPA-OS, http://sourceforge.net/projects/fipa-os/files/
7. Grasshopper, http://www.ikv.de/products/grasshopper

8. JADE, http://jade.cselt.it/
9. Nwana, H.S., Ndumu, D.T., Lee, L.C., Heath, M.: Zeus: An advanced tool-kit for engineering distributed multi-agent systems (1998)
10. DASH, http://www.agent-town.com/dash/index.html
11. Kawamura, T., Tahara, Y., Hasegawa, T., Ohsuga, A., Honiden, S.: Bee-gent:bonding and encapsulation enhancement agent framework for development of distributed systems. The transactions of the Institute of Electronics, Information and Communication Engineers D-I 82(9), 1165–1180 (1999)
12. Fujita, S., Hara, H., Sugawara, K., Kinoshita, T., Shiratori, N.: Agent-based design model of adaptive distributed systems. Applied Intelligence 9(1), 57–70 (1998)

An Effective Inference Method Using Sensor Data for Symbiotic Healthcare Support System

Satoru Izumi[1,2,4], Yusuke Kobayashi[1,2], Hideyuki Takahashi[1], Takuo Suganuma[1,2], Tetsuo Kinoshita[2,3], and Norio Shiratori[1,2]

[1] Research Institute of Electrical Communication, Tohoku University
[2] Graduate School of Information Sciences, Tohoku University
[3] Cyberscience Center, Tohoku University
[4] Research Fellow of the Japan Society for the Promotion of Science
2-1-1 Katahira, Aoba-ku, Sendai 980-8577, Japan
izumi@ka.riec.tohoku.ac.jp,
{kobayashi,hideyuki,suganuma,norio}@shiratori.riec.tohoku.ac.jp,
kino@riec.tohoku.ac.jp

Abstract. We have been investigating a symbiotic healthcare support system in ubiquitous computing environment. By using knowledge about healthcare and various kinds of information including vital sign, location information, and multimedia data of multiple object persons under observation of real world, the system provides useful information regarding health condition effectively and in user-oriented manner. This paper focuses on effective and real-time service provisioning using the information. The data and information including vital sign, location information, environmental information, multimedia data, specialized knowledge, etc. contain significant diverse aspects in both quantitative and qualitative. By using existing inference mechanisms, we cannot cope with these kinds of information and knowledge in real-time. In this work, we present an effective inference mechanism combining various kinds of sensor data and huge amount of knowledge on healthcare for providing healthcare information and services in real time.

Keywords: Sensor data, Ontology, Healthcare support system, Symbiotic computing.

1 Introduction

Unhealthy lifestyle produces obesity, hypertension, diabetes and hyperlipidemia, which are risk factors for heart diseases and cardiovascular diseases. Therefore these risk factors are generally called lifestyle-related diseases. In order to prevent them, people should exercise periodically and should change their lifestyle including meal, alcohol drinking and smoking. There are many health services that make lifestyle healthier based on information technologies [1,2,3]. For example, there are the health management systems which measure vital data using wearable sensors and store the data into a database (DB) for healthcare maintenance [4]. In [5], authors have developed a user interface in a mobile device

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 152–163, 2010.

to keep user's motivation. However, the existing healthcare systems acquire and manage only vital data of the user, and provide common healthcare information to the user only when the user requests.

We have been doing research on a symbiotic healthcare support system based on a concept of the symbiotic computing [6,7,8]. By using knowledge about healthcare and various kinds of information including vital sign, location information, and multimedia data of multiple object persons under observation of real world, the system provides useful information regarding health condition effectively and in user-oriented manner.

This paper focuses on effective and real-time service provisioning using the information. The data and information including vital sign, location information, environmental information, multimedia data, specialized knowledge, etc. contain significant diverse aspects in both quantitative and qualitative. By using existing inference mechanisms, we cannot cope with these kinds of information and knowledge in real-time. In this paper, we present an effective inference mechanism combining various kinds of sensor data and huge amount of knowledge on healthcare for actively-provisioning in real-time. In this paper, especially, we propose a knowledge filtering method based on sensor data.

2 Relates Works and Problems

2.1 Related Works

Research on Effective Method of Sensor Data Processing
There are researches that define universal sensor ontologies to search distributed and heterogeneous sensor data [9,10,11]. They have given methods for provide sensor data according to user's query.

The Semantic Sensor Network has been proposed for common use of sensor data by several applications [12]. This is a middleware that connects the variety of physically grounded applications to the information of the real world. The middleware infers and describes the state of an environment using logical expressions so as to construct efficiently an interpretation model for sensor data and queries.

Moreover, the JUSTO, the inference system which works on logical representations provided by the Semantic Sensor Network has been proposed [13]. Since inferences from changed logical representations are erased immediately, the JUSTO is able to correspond dynamic change on logical representations. The JUSTO can make the inference suited to real world environment, which is dynamically changing environment. In addition, JUSTO's inference algorithm can generate the expression based on stable logical representations.

Research on Effective Method of Knowledge Processing
On the other hand, the paper [14] focused on effective method of knowledge processing. Specifically, this paper proposes a knowledge-filtering agent, which quickly responds the query by dynamic classification of the useful information along with the user context (e.g., time, place, occasion, and personalization) changing in the real world.

2.2 Problems

From the related works described above, we point out technical problem that it is difficult to provide an advanced service combining many kinds of sensor data and huge amount of knowledge in real time. By utilizing many kinds of sensor data such as vital sign, location data, temperature, humidity, acceleration, and multimedia data and huge amount of knowledge, the system can provide an advanced services. However, the existing researches have focused on either processing of sensor data or that of knowledge. Thus, these researches have the limitation of inference processing for provisioning services combining huge amount of knowledge and many kinds of sensor data in real time. Therefore, it is required to efficiently process both sensor data and knowledge for timely and useful service-provisioning.

3 Proposal: An Effective Inference Mechanism Using Sensor Data

3.1 Applying Ontology

To overcome the problem described in section 2.2, we propose an effective inference mechanism using sensor data. In order to provide an advanced healthcare services and advices under considering user's condition and privacy, it is important that a healthcare support system needs to recognize situation such as vital data of user and environmental information along with the user context changing in the real world. The system also must recognize knowledge about healthcare such as user's constitution and lifestyle habit, an effect of each exercise, and an effective meal for each disease.

Moreover, when the system informs the user's status to not only the user but also the user's community including family, doctor, instructor, etc., the system should keep the user's privacy according to the human relationships between the user and the community members, and derive the information with an appropriate form at the right time.

The Semantic Web technology [15,16] may provide a solution for the above problem. In the Semantic Web technology, meta-data is added to various types of information resources and they are classified and/or aggregated based on an ontology [17] which represents knowledge concepts formally. By using their meta-data and an ontology, a software can understand a user context and the semantics of heterogeneous information resources. Therefore the software provides a richer service to the user. The system can derive adequate advices according to user's health condition because an ontology is introduced into the system for describing the knowledge about exercise, lifestyle and user's health condition. The knowledge contents are associated by the ontology and the associations show the semantic map of the knowledge contents. It helps the system to understand what service or advice is good for user's request and health condition.

3.2 Effective Inference Method Combining Sensor Data and Ontology

The effective inference method combining the ontology and sensor data, has two phases. One is an ontology filtering phase based on user's and resource's situations, the other is a dynamic control phase on frequency of sensor data acquisition.

Ontology Filtering Phase Based on User's and Resource's Situations This phase filters the knowledge (ontology) based on user's situation to cope with huge amount of knowledge effectively. The system may have huge amount of knowledge about healthcare for advanced service provisioning, but it is difficult to meet the user's real-time query. Therefore, it is required to retrieve timely and useful piece of the knowledge from huge amount of knowledge about healthcare according to the user and resource situations.

Thus, we propose an ontology-filtering method to quickly responds the user's request by dynamic classification of the useful information along with the user context changing in the real world. For example, based on user's lifestyle habit expressed by extended temporal ontology [18], the system extracts a piece of knowledge for service provision from the whole ontology. Or, when the user moves to the room, the system extracts the knowledge related to the room where the user is (e.g., the environmental sensor in the room, and the activity which should be done in the room) The extracted ontology is used for real time service provisioning, e.g., to infer the user's health condition. This meets effective inference process using huge mount of knowledge.

Dynamic Control Phase on Frequency of Sensor Data Acquisition This phase can dynamically control frequency of sensor data acquisition based on the user's health condition. If many kinds of sensor data (e.g., vital sign, environmental data, multimedia data) flow to the system, its performance may decrease. This phase is possible to solve the problem. Specifically, the system analyze the user's health condition and tend from vital data in the database by using data stream mining technology in real time. If the system detects the aberration of user's normal condition, the system gets the user's vital sign and user's surround information (e.g., temperature, and humidity) from the corresponding vital sensors and environmental sensor in shorter time intervals, and the other senors' frequency of data acquisition is decreased. This makes the system infer the user's condition and advice effectively keeping quality of derived service and advice.

3.3 Symbiotic Healthcare Support System Based on Multi-agent Technology

Applying proposed method to a healthcare support, we develop the symbiotic healthcare support system. Fig. 1 shows an overview of the system. In our system, system components such as vital sensors, sensor network, databases (DBs),

knowledge bases (KBs), and inference engines are wrapped, then theses components work as agents. The agents is capable of flexible autonomous action to meet its design objectives. They have the intelligence to react to situations, and they can act pro-actively and also may have some social abilities (e.g. negotiation) to achieve desired objectives.

To realize proposed effective inference method, senor agents, DB agents, KB agent, inference agent, data stream mining agent work as a multi-agent system, that is a distributed autonomous system. Each agents works cooperatively to do inference process for service provision.

Its overall concept, functions, and example behaviors are described in [19]. Therefore, we omit them here, and focus on the effect of the ontology filtering phase based on user's and resource's situations.

4 Experiment

4.1 Overview

We performed experiments by using the prototype system to confirm the effectiveness of the ontology filtering phase based on user's and resource's situations.

Our prototype system gets location and environmental data from sensors in real world. Then the system infers user's situation utilizing the sensor data and

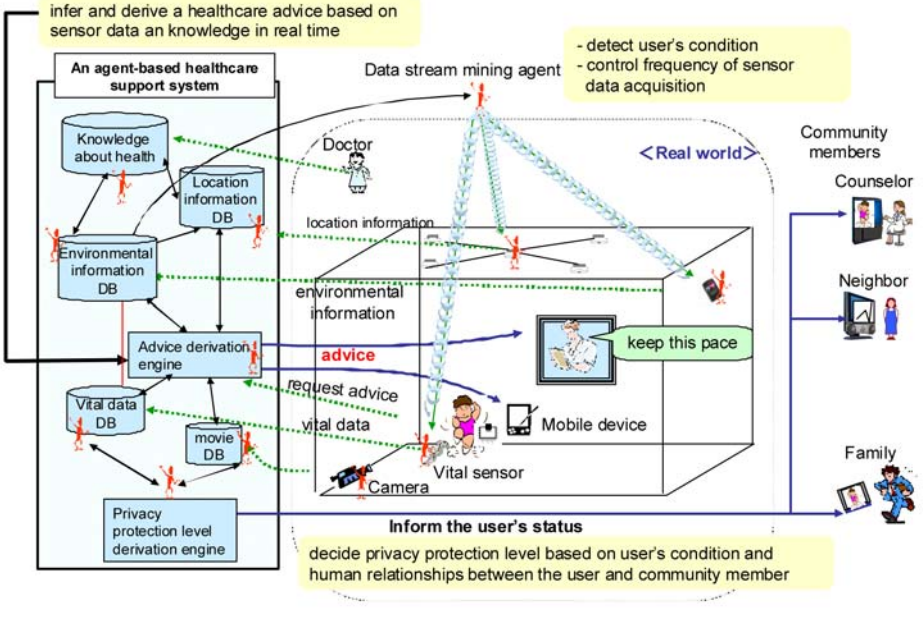


Fig. 1. Overview of symbiotic healthcare support system

Table 1. Performance of PC (inference engine)

CPU	Memory	OS
Intel (R) Core 2 Duo 2.66GHz	4GB	Windows Vista

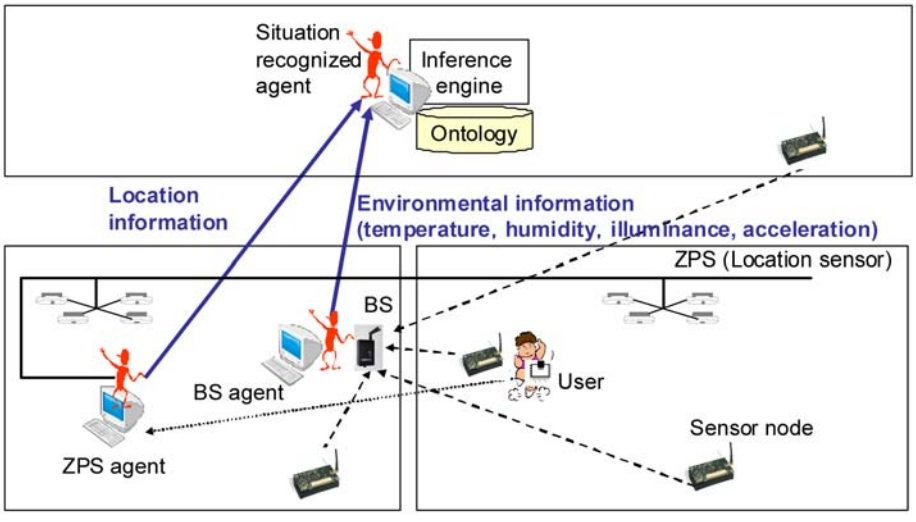


Fig. 2. Experimental environment

the knowledge about healthcare. We measured inference time to derive the user's situation.

4.2 Experimental Environment

Fig. 2 shows our experimental environment. We use MOTE (MTS310) [20] as an environmental sensor. This sensor measures temperature, brightness, acceleration, and magnetism. To get user's location, we use ultrasonic sensor: Furukawa's Zone Positioning System (ZPS) [21]. For the agent implementation, we use DASH [22], a multi-agent-based programming environment and IDEA [23], an integrated development tool for the DASH. For describing an ontology and inference rules, we use Web Ontology Language (OWL) [24] and Semantic Web Rule Language (SWRL) [25], respectively. To filter an ontology and execute inference based on the ontology, we use Jena [26]. Table 1 shows the performance of PC for inference engine, and Table 2 expresses size of knowledge.

4.3 Knowledge about Healthcare Support

We explain knowledge (ontology) about healthcare support. Fig. 3 shows our ontology for our experiments. In this figure, an an oval represents a concept (class)

Table 2. Number of class, instance, and inference rule of knowledge

Class	Instance	Inference rule
67	95	40

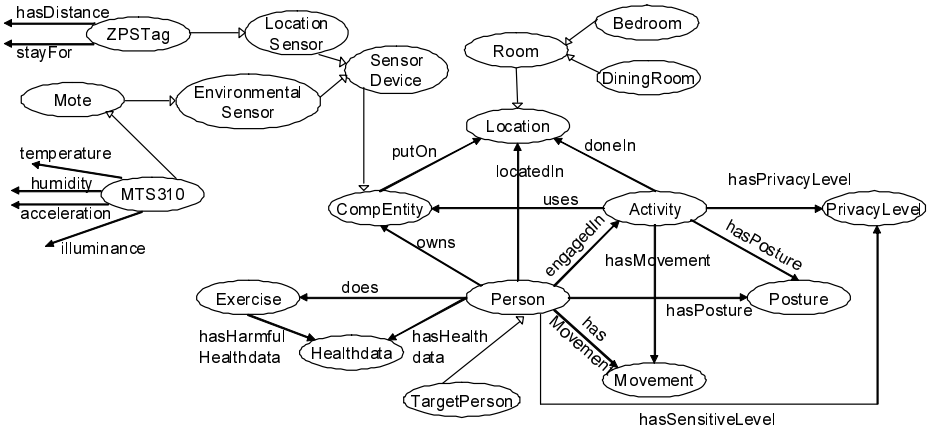


Fig. 3. Top level of ontology about healthcare support

and an arrow represents a relationship (property) between classes. Focusing on healthcare domain, we extended and detailed this ontology based on a context ontology defined in [27]. The following kinds of knowledge are expressed in our ontology.

- Relationship between a person and a location (e.g., a user A is in dining room.)
- Relationship between the person and a device (e.g., the user A has location tag whose ID is 28.)
- Relationship between the location and an activity (e.g., bedroom is a room for sleeping.)
- Relationship between the activity and a posture (e.g., when a person is sleeping, the person is lying.)

This ontology expresses concepts of healthcare support and their relationships. Our healthcare support system can derive user's situation combining the ontology and inference rules. One of the inference rules we defined is as follows.

own(?user, ?locationTag) ∧
putOn(?locationTag, ?room)
→ locatedIn(?user, ?room)

This rule means "if a user has a location sensor tag, and the tag is in a room, then the user is located in the room."

The following rule derives the user's posture from value of location sensor tag.

own(?user, ?locationTag) ∧
distance(?locationTag, ?distance) ∧
(?distance < 100) ∧
stayFor(?locationTag, ?stay) ∧ (?stay > 60)
→ hasPosture(?user, lying)

This rule shows "a user has a location sensor tag, the height of the tag is less than 100 mm, and the staying time of the tag is more than 60 seconds, then the user is lying."

The following rule derives user's movement from acceleration.

own(?user, ?environmentalSensor) ∧
acceleration(?environmentalSensor, ?acceleration)
∧ (?acceleration == 0) ∧
stayFor(?environmentalSensor, ?stay) ∧
(?stay > 60)
→ hasMovement(?user, stop)

The above rule expressed "a user has a environmental sensor, the acceleration of the sensor is 0, and the staying time of the value is more than 60 seconds, then the user is stopping."

The following rule derives user's activity according to the room where the user is, user's activity and movement.

locatedIn(?user, ?room) ∧
doneIn(?room, ?activity) ∧
hasPosture(?user, ?posture) ∧
hasPosture(?activity, ?posture) ∧
hasMovement(?user, ?movement) ∧
hasMovement(?activity, ?movement)
→ engagedIn(?user, ?activity)

This rule explains "a user is in a room, there is an activity which should be done in the room, there is a posture and a movement a person takes when the person does the activity, and the user actually takes the posture and the movement, then the user takes the activity." Our system derives user's actually activity and situation based on the ontology, inference rules, and sensor data from real world. For example, we assume the user's situation, "the user is sleeping in the bed room." From the location sensor data and environmental sensor data, the system can recognize user's actual posture and movement. In this case, "the user is lying and stopping in the bed room." is derived. Then, because the social knowledge "The bed room is a room for sleeping and when a person is sleeping, the person is lying and stopping." is expressed by our ontology and inference rules, our system can understand "the user is sleeping in the bed room normally."

Moreover, to derive various user's situations, we equip some rules. For example the following rules are equipped.

– A user has a location tag and environmental sensor, location tag is low position in the bed room, acceleration changes frequently, and illuminance in the room is low → the user is lying in the bed and moving.
– A user has a location tag and environmental sensor, location tag is high position in the dining room, and acceleration changes frequently → the user takes activity in the dining room.

4.4 Scenarios

We equip three environmental sensor nodes, and set them in each room. A user also has one environmental senor node to detect user's movement from acceleration. Each sensor measures temperature, illuminance, acceleration etc. once a second, then sends these sensor data to a base station (BS) agent. When the BS agent gets sensor data, it sends the data to a situation recognized agent. A ZPS agent also gets location data once a second, then sends it to the situation recognized agent. When the user moves to the room, the situation recognized agent executes the ontology filtering based on the user's location. Fig. 4 shows an example of the filtering method based on user's location. In this figure, a square shows an individual (instance) of a class. When the user A moves to the room w315, and stays there, the situation recognized agent extracts the ontology related user's room is extracted from the whole ontology including huge amount information (e.g., all sensor nodes information related the user A). Then, the situation recognized agent infers the user's situation based on the extracted ontology and received sensor data using an inference engine. We measured inference time to derive the user's situation using sensor data.

4.5 Experimental Result

Table 3 shows experimental results. Each value means average inference time (ms). We used four sensor nodes and each node measures environmental data once a second. Thus, the situation recognized agent gets 4 sensor data per second from the BS agent. Therefore, the situation recognized agent needs to process these data within 250 ms. From the Table 3, in the case of the existing method, the agent cannot process these sensor data within 250 ms, On the other hand, in the case of proposed method, By filtering the ontology, the extracted ontology was reduced to 19 classes and 25 instances. Thus, the agent can cope with sensor data. Therefore the agent can infer the user's situation in real time.

This results show that existing inference method cannot cope with many kinds of sensor data and huge amount of knowledge, and by extracting knowledge from huge amount of knowledge, we can detect user's situation quickly.

Table 3. Experimental Results : Inference time (ms)

	Existing method (no filtering)	Proposed method (filtering)
Inference time	1118	103

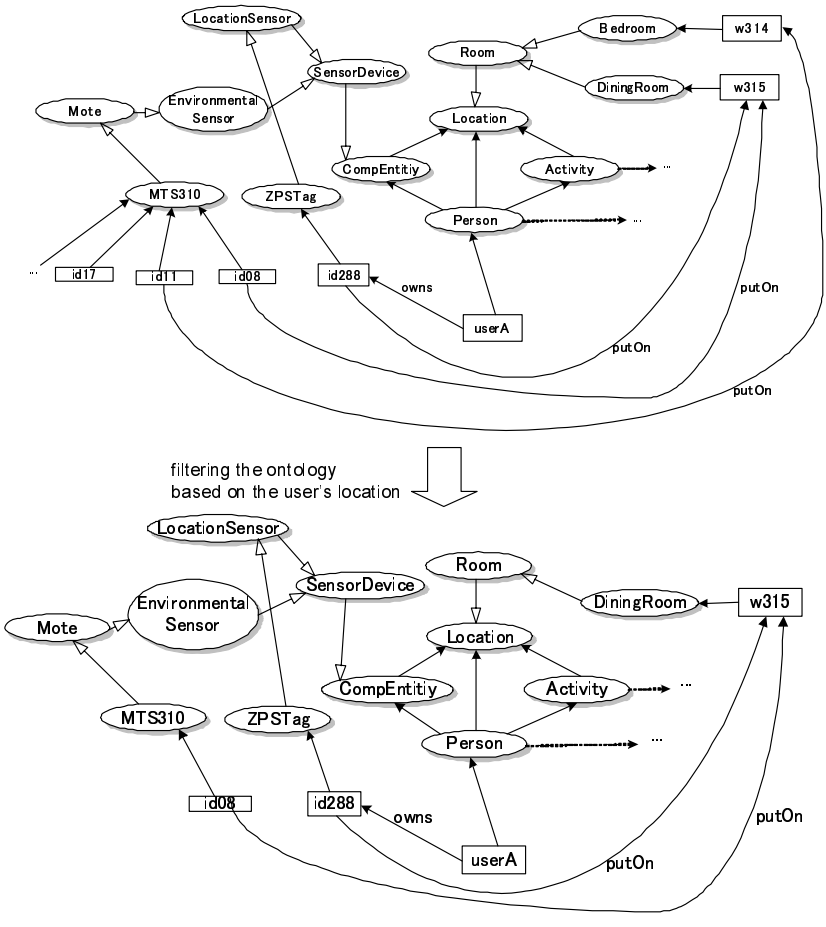


Fig. 4. Filtering method

5 Conclusion

In this paper, we propose an effective inference method combining various kinds of sensor data and huge amount of knowledge on healthcare for providing healthcare information and services in real time. Especially, we propose an ontology filtering method based on sensor data.

Our future work includes the detailed design and implementation of proposed filtering method, and its evaluation. We will develop the our healthcare support system with our proposed method.

Acknowledgement

This work was partially supported by Sendai Intelligent Knowledge Cluster, the Ministry of Education, Culture, Sports, Science and Technology, Grants-in-Aid for Scientific Research, 19200005, and the Grant-in-Aid for JSPS Fellows No.21007220 of Japan Society for the Promotion of Science (JSPS).

References

1. http://www.mhlw.go.jp/bunya/kenkou/index.html
2. Leijdekkers, P., Gay, V., Barin, E.: Trial Results of a Novel Cardiac Rhythm Management System Using Smart Phones and Wireless ECG Sensors. In: Mokhtari, M., Khalil, I., Bauchet, J., Zhang, D., Nugent, C. (eds.) ICOST 2009. LNCS, vol. 5597, pp. 32–39. Springer, Heidelberg (2009)
3. Ouchi, K., Suzuki, T., Doi, M.: LifeMinder: A Wearable Healthcare Support System with Timely Instruction Based on the User's Context. IEICE Transactions on Information & Systems E87-D(6), 1361–1369 (2004)
4. Kuriyama, D., Izumi, S., Kimura, S., Ebihara, Y., Takahashi, K., Kato, Y.: Design and Implementation of a Health Management Support System Using Ontology. In: Proceedings of the International Conference on Engineering, Applied Sciences, and Technology (ICEAST 2007), pp. 746–749 (2007)
5. Kudlacz, M., Tan, R., Prindiville, J., Peters, M.: RoutePlanner. In: Proceedings of Conference on Human Factors in Computing Systems (CHI 2006), pp. 1849–1854 (2006)
6. Symbiotic Computing Home Page, http://symbiotic.agent-town.com/
7. Suganuma, T., Sugawara, K., Shiratori, N.: Symbiotic Computing: Concept, Architecture and Its Applications. In: Indulska, J., Ma, J., Yang, L.T., Ungerer, T., Cao, J. (eds.) UIC 2007. LNCS, vol. 4611, pp. 1034–1045. Springer, Heidelberg (2007)
8. Suganuma, T., Uchiya, T., Konno, S., Kitagata, G., Hara, H., Fujita, S., Kinoshita, T., Sugawara, K., Shiratori, N.: Bridging the E-Gaps: Towards Post-Ubiquitous Computing. In: Proceedings of the 1st International Symposium on Frontiers in Networking with Applications (FINA 2006), pp. 480–484 (2006)
9. Kim, J.H., Kwon, H., Kim, D.H., Kwak, H.Y., Lee, S.J.: Building a Service-Oriented Ontology for Wireless Sensor Networks. In: Proceedings of the 7th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2008), pp. 649–654 (2008)
10. Eid, M., Liscano, R., Saddik, A.E.: A Novel Ontology for Sensor Networks Data. In: Proceedings of the IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA 2006), pp. 75–79 (2006)
11. Eid, M., Liscano, R., Saddik, A.E.: A Universal Ontology for Sensor Networks Data. In: Proceedings of the IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA 2007), pp. 59–62 (2007)
12. Hirota, Y., Kawashima, H., Umezawa, T., Imai, M.: Design and Implementation of Real World Oriented Metadata Management System MeT for Semantic Sensor Network. The IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences J89-A(12), 1090–1103 (2006)

13. Kanda, T., Satake, S., Kawashima, H., Nakamura, M.: JUSTO: An Inference System on Semantic Sensor Network. In: Proceedings of the 20th Annual Japanese Conference on Artificial Intelligence (2006)
14. Takenouchi, T., Okamoto, N., Kawamura, T., Ohsuga, A., Maekawa, M.: Development of Knowledge-Filtering Agent along with User Context in Ubiquitous Environment. IEICE Transaction on Information and Systems J88-D1(9), 1428–1437 (2005)
15. W3C Semantic Web Activity, http://www.w3.org/2001/sw/
16. Berners-Lee, T.: Semantic Web Road Map, http://www.w3.org/DesignIssues/Semantic.html
17. Staab, S., Studer, R.: Handbook on Ontologies. Springer, Heidelberg (2004)
18. Izumi, S., Yamanaka, K., Tokairin, Y., Takahashi, H., Suganuma, T., Shiratori, N.: Ubiquitous Supervisory System based on Social Contexts using Ontology. Mobile Information Systems (MIS) 5(2), 141–163 (2009)
19. Takahashi, H., Izumi, S., Suganuma, T., Kinoshita, T., Shiratori, N.: Design and Implementation of Healthcare Support System based on Agent-based Framework. In: Proceedings of The 4th International Conference on Ubiquitous Information Technologies & Applications (ICUT2009), pp. 213–218 (2009)
20. http://www.xbow.jp/motemica.html
21. Zone Positioning System, http://www.furukawakk.jp/products/
22. Sugawara, K., Hara, H., Kinoshita, T., Uchiya, T.: Flexible Distributed Agent System programmed by a Rule-based Language. In: Proceedings of the 6th IASTED International Conference of Artificial Intelligence and Soft Computing, pp. 7–12 (2002)
23. Uchiya, T., Maemura, T., Hara, H., Sugawara, K., Kinoshita, T.: Interactive Design Method of Agent System for Symbiotic Computing. International Journal of Cognitive Informatics and Natural Intelligence 3(1), 57–74 (2009)
24. OWL Web Ontology Language Reference, http://www.w3.org/TR/owl-ref
25. SWRL: a Semantic Web Rule Language Combining OWL and RuleML, http://www.daml.org/2003/11/swrl/
26. Jena – A Semantic Web Framework for Java, http://jena.sourceforge.net/
27. Gua, T., Pung, H.K., Zhang, D.Q.: A service-oriented middleware for building context-aware services. Journal of Network and Computer Applications 28(1), 1–18 (2005)

3D Collaboration Environment Based on Real Space and Digital Space Symbiosis

Gen Kitagata[1], Akira Sakatoku[2], Akifumi Kawato[2], Toshiaki Osada[1], Tetsuo Kinoshita[3], and Norio Shiratori[1]

[1] Research Institute of Electrical Communication, Tohoku University, Katahira 2-1-1, Aoba-ku, Sendai, Miyagi, Japan
[2] Graduate School of Information Sciences, Tohoku University, Aramaki aza Aoba 6-3-09, Aoba-ku, Sendai, Miyagi, Japan
[3] Cyberscience Center, Tohoku University, Aramaki Aza Aoba 6-3, Aoba-ku, Sendai, Miyagi, Japan

Abstract. In this paper, we propose 3D symbiotic collaboration environment which is based on concept of real and digital spaces symbiosis. Collaboration environments which are using Augmented Reality have been expected to realize effective collaborative works. However, the construction of these environments has a limitation, because devices which do not have an ability of sensing the real-space information cannot be used for these environments. To break this limitation, we propose the 3D symbiotic collaboration environment which enables users to do collaborative works intuitively as if 3D digital spaces united with the real space. In this paper, we present fundamental technologies for 3D symbiotic collaboration environment. In addition, we show the design and implementation of the prototype system, and confirm feasibility of 3D symbiotic collaboration environment with experimental results of the prototype system.

1 Introduction

In traditional ubiquitous information environments, co-recognition with the real world, such as the suitable sensing of information or the provision of services as suitable forms, is insufficiently. Therefore, the capability of these environments cannot be sufficiently utilized for the real world. Aiming towards the next generation ubiquitous information environment which overcomes this issue, the concept of "Symbiotic Computing" [2] has been advocated. Symbiotic Computing is to realize co-recognition between the real world and ubiquitous information environments, and integrates them together effectively.

Collaborative work environments also have insufficient co-recognition with the real world. Collaborative work environments which applied Mixed Reality [6] have such co-recognition, and these environments are expected to realize effective collaborative works. However, the architecture of these environments cannot realize such co-recognition at devices which are unevenly distributed in the real world. Consequently, the construction of these environments is limited. This limitation causes the gaps between the real space and digital spaces, and it make users unable to work intuitively.

To solve this problem, we propose 3D symbiotic collaboration environment which is based on concept of real and digital spaces symbiosis. 3D symbiotic collaboration

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 164–174, 2010.

environment is a collaborative work environment based on Symbiotic Computing in which agent based applications, traditional applications and users work together. We aim to break a limitation in the construction of these environments. 3D symbiotic collaboration environment will bridge the gaps between the real space and digital spaces, and enable to construct an intuitive collaborative work environment. In this paper, we present fundamental technologies for 3D symbiotic collaboration environment.

The remainder of the paper is organized as follows. In Section 2, we explain related works. In Section 3, we propose the construction scheme of 3D symbiotic environment. Then we present the design and implementation of the prototype system in Section 4. Subsequently, we confirmed feasibility of 3D symbiotic environment with experimental results of the prototype system in Section 5. Finally in Section 6, we conclude this paper.

2 Related Works

2.1 Augmented Reality

Augmented Reality (AR) is a technology which enables to superimpose digital spaces on the real space. Collaborative work environments based on AR [1,7] have been developed until now. These researches substantiated the effectiveness of introducing AR to collaborative works. However, in the architecture of these environments, the real-space information, which is used in AR, is sensed by each individual device. Thus, devices which do not have an ability of sensing the real-space information cannot be used for these environments. if such devices were placed in a collaborative work environment, the gaps arise between the real space and digital spaces, such as a limitation of the positions where users can use this environment. These gaps lower the realistic sensation of collaborative work environments, and make users unable to work intuitively.

2.2 User Interface

Usual collaboration environment applying Virtual Reality are focused on 3D interaction based collaborative works, e.g. collaborative design system or communication system utilizing 3D objects in digital space. Users can do such collaborative works intuitively as if they are working in real space. However, these collaborative environments have a limitation of flexibility because they are designed for a certain task.

The limitation can be eased by using 3D user interface[5]. 3D user interface extends traditional 2D interface to 3D. That is to say, by utilizing 3D interface, we can use traditional applications via 3D interaction. However, these applications can be interact within a certain collaborative environment, and it can not interact with other collaborative environments. For example, even if we give 3D user interface to an agent based application, the agent can not join other collaborative works, so it is not effective.

2.3 Problems

As mentioned in Section 2.1, the applicable scope of traditional collaborative work environments based on AR is limited, because an ability of sensing the real-space information is required for devices. Thus, a scheme which circulates the real-space information

to several devices is necessary. Moreover, as mentioned in Section 2.2, it is difficult for applications to collaborate with 3D interaction based collaborative works effectively. Thus, we need scheme to integrate many types of applications including agent based applications to 3D interaction based collaborative works.

From the above, there are the following issues to construct an intuitive collaborative work environment: the circulation of the real-space information to several devices, and integration of many types of applications into 3D interaction based collaborative works.

3 3D Symbiotic Collaboration Environment

3.1 Outline of Proposal

In this paper, we propose the 3D symbiotic collaboration environment based on Real and Digital Spaces symbiosis and its construction scheme. 3D symbiotic collaboration environment is a fundamental technology to solve problems as mentioned in Section 2.3, and to construct the intuitive collaborative work environment. Our proposal is consists of the following two schemes:

(S1) Real-Space Information Circulation Scheme: This scheme circulates the real-space information to several devices. It enables to bridge the gaps between the real space and digital spaces and to construct an intuitive collaborative work environment.

(S2) Application Composition Scheme Based on the Tool Metaphor: This scheme composes agents and applications based on the metaphor of tools in the real space. It enables these applications to integrate with 3D interaction based collaborative works.

In Section 3.2 and 3.3, we describe the details of (S1) and (S2), respectively.

3.2 Real-Space Information Circulation Scheme

To construct 3D symbiotic collaboration environment, we circulate real-space information by circulation scheme. In addition, we show the seamless convergence of the real space and digital spaces according to these information. We use display terminals as display devices, and use their physical positions in the real space as the real-space information. Fig.1 shows an outline of this scheme.

The real-space information is sensed and circulated to several devices in the real space. To sense the positions as the real-space information, markers are placed at various places in the real space such as display terminals. And then, the positions of markers are analyzed by the camera image of the real space. These positions are sent to each display terminal.

According to the real-space information which is circulated, the seamless convergence of the real space and digital spaces is controlled. To control the seamless convergence, digital spaces which are superimposed on the real space are created beforehand. When display terminals received the positions, the viewpoint of digital spaces on each display terminal is controlled according to received positions and parameters of the superimposition. Specifically, a position and a direction in digital spaces are computed

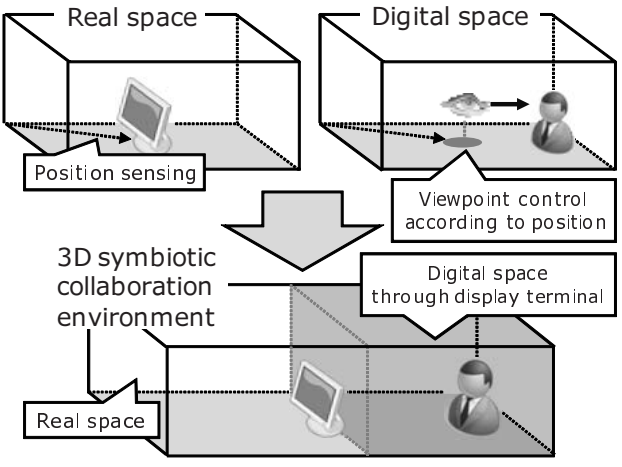


Fig. 1. An outline of real-space information circulation scheme

corresponding to a position and a direction in the real space, and also the viewpoint is changed according to computed results.

This scheme enables to show digital spaces which are superimposed on the real space, as looking through display terminals in the real space. That is, the seamless convergence of the real space and digital spaces is represented effectively, and it enables users to use digital spaces as if they are united with the real space.

3.3 Application Composition Scheme Based on the Tool Metaphor

To realize the effective application composition in the 3D symbiotic collaboration environment, we compose applications based on the metaphor of tools in the real space. In the real space, we usually use a tool by combining with another tool. For example, a pen is used with a paper and vice versa. In this case, the function of writing is depended on the pen, i.e. colors of lines are changed by changing the pen. On the other hand, properties of the document are depended on the paper. We define these characteristics as a model of tools as follows:

When a "physical event" occurred between one tool and another, a "function" of the tool will be transmitted to another one and it produces an effect.

In this definition, the physical event means a mechanical interaction which works between one object and another. Furthermore, the function is an effect which is given to one tool from another.

In this scheme, the application is represented as the object in 3D symbiotic collaboration environment to define the above-mentioned physical event at the application, and the occurrence of physical events are checked by the environment. In this paper, the following mechanical interactions are considered as a part of physical events.

- An object approaches to a part of the object.
- An object touches a part of the object.
- An object points at a part of the object.

Also we define a function as a program which has input and output as follows:

Input: Parameters of the physical event
Output: Modification of variants in the destination object

The proposed scheme works according to a process as follows: First, users manipulate objects, and the occurrence of physical events between objects is checked by the environment. When the environment detects physical event, the source object and the destination object are decided according to this event. Next, the function of the source object was transmitted to the destination object. Finally, the destination object produces an effect of function on itself.

This scheme enables users to do collaborative works in digital spaces intuitively as if they are using tools in the real space. That is, this scheme realizes the functional level cooperation based on the function of the application object, and it has high affinity with the real space by the physical event.

4 Design and Implementation

4.1 System Architecture

We design and implement the prototype system to confirm feasibility of our proposal. The prototype system consists of five types of elements as follows:

[Symbiotic Environment Server]. This server constructs digital spaces. Furthermore, The server decides the viewpoint on symbiotic environment clients from the positions of display terminals which is sensed by the sensor server, and circulates them to each symbiotic environment clients. In addition, the server processes manipulation requests from symbiotic environment clients, and mediates the functions of application which are transmitted by application servers.

[Sensor Server]. This server senses the positions of display terminals from the camera image. These positions are sent to the symbiotic environment server.

[Application Server]. This server sends their function in accordance with requests. When the server received a function, the server produces the effect of function on target application, and requests a modification of 3D symbiotic environment if necessary.

[Symbiotic Environment Client]. This client is running on a display terminal, and shows 3D symbiotic environment view which is constructed by the symbiotic environment server. In addition, the client requests manipulation of 3D symbiotic environment to the symbiotic environment server.

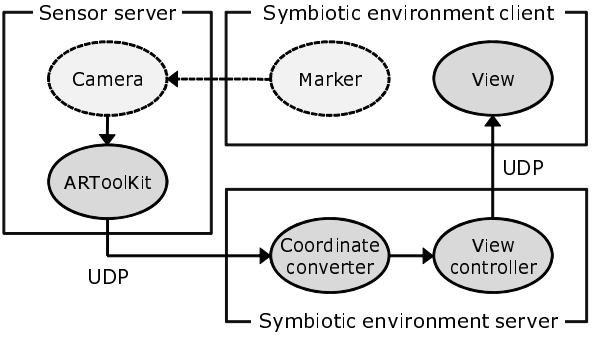


Fig. 2. An outline of the 3D symbiotic environment control

4.2 3D Symbiotic Environment Control Process

Fig.2 shows an outline of the 3D symbiotic environment control. The positions of display terminals in the real space are sensed by using ARToolKit [4]. ARToolKit is a library which is useful for creating applications with AR. First, it is necessary to connect a video camera to the sensor server, to obtain a camera image. Next, the sensor server analyzes the camera image by using ARToolKit, and senses the relational positions of display terminals from the video camera. Finally, the server sends these positions to the symbiotic environment server.

In the symbiotic environment server, at first, it computes the absolute positions of display terminals according to two information as follows: the relational positions which is received from sensor server, and the parameters of the superimposition which are set beforehand. Next, the server decides the viewpoint of digital spaces according to the absolute position. Finally, the server gives notice of this viewpoint to symbiotic environment clients, and makes these clients to be reflected this viewpoint.

4.3 Application Composition Process

Fig.3 shows a sequence chart of the application composition. First, descriptions of correspondence between the application and the object in 3D symbiotic environment are prepared. Secondly, the symbiotic environment server request to start application to application servers, according to these descriptions. When users manipulated an object of application, as shown in Fig.3 ·1), the symbiotic environment server checks whether a physical event is occurred on this object or not, as shown in Fig.3 ·2). If the physical event was detected, the symbiotic environment server mediates the function of the application from the source application to the destination application, as shown in Fig.3 ·3). The destination application produces the effect of function on itself, as shown in Fig.3 ·4). In addition, these applications can request a modification of 3D symbiotic environment, like a modification of the position of the object, the model of the object, or the texture of the object, as an output, as shown in Fig.3 ·5). This output is shared by the symbiotic environment server among symbiotic environment clients, as shown in Fig.3 ·6).

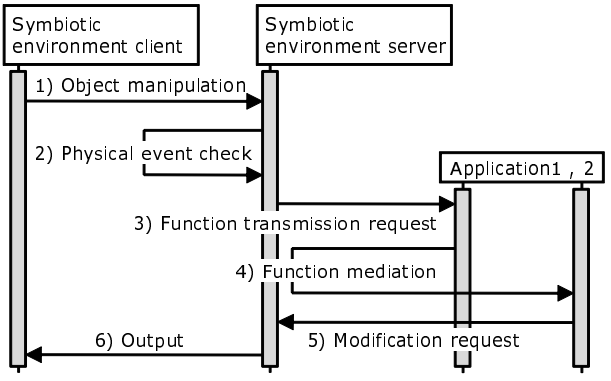


Fig. 3. A sequence chart of the application composition

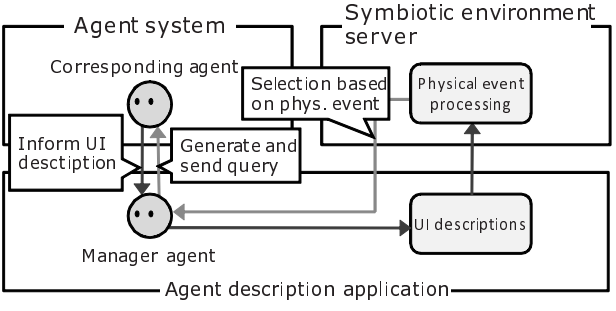


Fig. 4. Flow of agent's UI description

4.4 Agent Composition Process

To integrate agent based applications into physical event based environment, we introduce user interface (UI) description for agent. Flow of agent's UI description are shown in Fig.4.

First, an agent inform its UI description to manager agent. The UI description is aggregated in the manager agent, then the description is realized as UI object in symbiotic environment server via agent description application. Also the agent description application makes query according to physical event received by the environment, and sends the event to corresponding agent.

Each agent in agent system makes UI description according to its capability of query processing. For instance, the agent makes candidates of query parameters which can be processed beforehand, and the agent is needed to substantialize UI to select parameters.

Fig.5 shows an example of UI description of DASH agent. Fig.5 ·(a) is an example of UI description. Query parameters mentioned above are described as candidate list. The manager agent generates UI for candidate selection. When an item in the list are selected, query described in Fig.5 ·(b) is generated and sent to corresponding agent according to selection result.

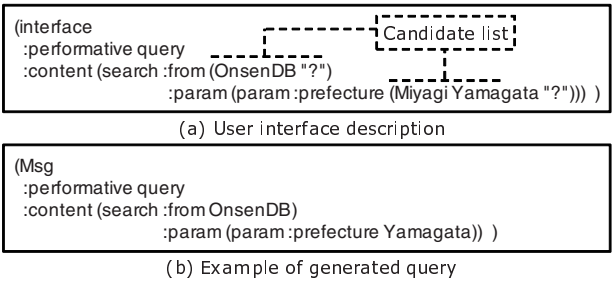


Fig. 5. Example of agent's UI description

4.5 Implementation

We implement the prototype system based on the design as mentioned in above sections.

In this implementation, we use Java for the symbiotic server, application servers, the symbiotic environment clients, and use C language for the sensor server. Furthermore, we use DASH as agent platform[3].

5 Experiments and Evaluation

5.1 3D Symbiotic Environment Construction Experiments

We experimented with real-space information circulation scheme by using the prototype system.

Fig.6 shows a process of these experiments. We created a digital space with a car model as a digital space which is converged to the real space. On the other hand, we placed a display terminal as a symbiotic environment client, and a sensor server configured to sense the position of the display terminal, in the real space. We carried out

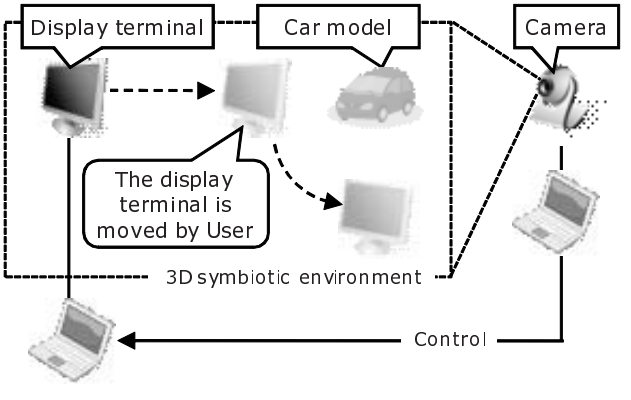
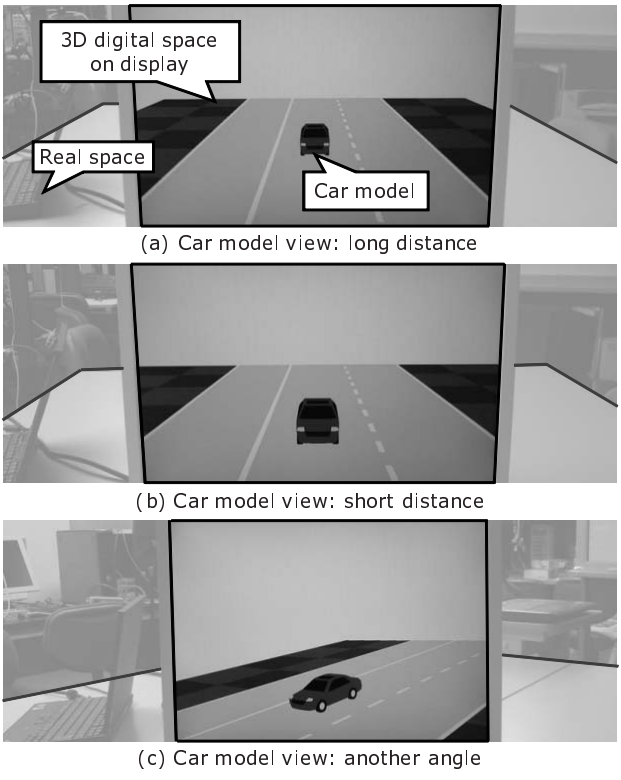


Fig. 6. A process of 3D symbiotic environment construction experiments



(a) Car model view: long distance

(b) Car model view: short distance

(c) Car model view: another angle

Fig. 7. Results of 3D symbiotic environment construction experiments

experiments to test the behavior of the proposed scheme when the display terminal was moved.

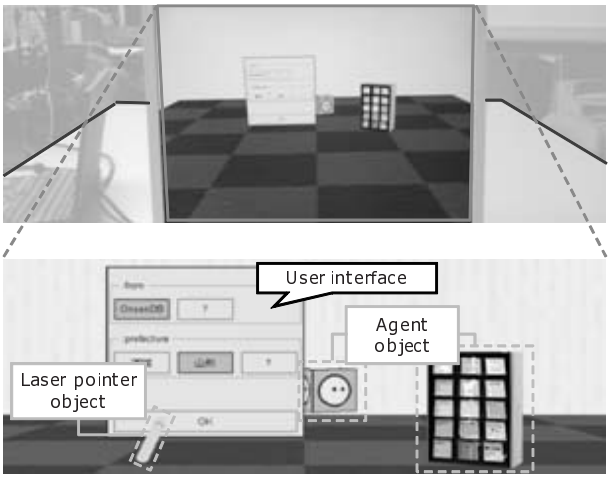
Fig.7 shows results of these experiments. The car model was shown on the symbiotic environment client, as shown in Fig.7 ·(a). We could show the car model as if it didn't move when the display terminal was moved back and forth, because the position of the display terminal was circulated to the client, as shown in Fig.7 ·(b). We could also show the car model around to the side of it, as shown in Fig.7 ·(c). That is, the car model which was superimposed on the real space was shown as looking through the display terminal in the real space.

Because our system captures camera image to sense location of objects in real space, delay time is exists. However, through the above experiments, delay time was around 200msec. We believe that this delay time is short enough for practical use.

5.2 Application and Agent Composition Experiments

We experimented with application composition scheme based on the tool metaphor by using the prototype system.

We introduced a a laser pointer application on digital spaces. This application have function which corresponded to a laser pointer in the real space. Additionally, we



(a) Agent and application behavior based on physical event.

(b) Result view of agent process

Fig. 8. Results of application and agent composition experiments

introduced data search agent via agent description application. This agent has a role to search data and output its results. We carried out experiments to test the behavior of the proposed scheme when users manipulated these applications.

Fig. 8 shows results of these experiments. When users manipulated the laser pointer object and pointed it to UI of agent, the function of the laser pointer was transmitted to agent via agent description application. That is, the agent based application and the laser pointer application were combined by physical event. Especially, user could use the laser pointer application as if it was in real space.

5.3 Evaluation

As the experiments indicated in Section 5.1, the digital space which is superimposed on the real space is shown as looking through the display terminal in the real space. From these experimental results, we confirmed that the seamless convergence of the real space and digital spaces is represented effectively. It enables users to use digital spaces as if digital spaces united with the real space.

Moreover, as the experiments indicated in Section 5.2, users could user data search agent intuitively by manipulating the laser pointer application. From these experimental

results, we confirmed that the proposed scheme can integrate many types of application including agent based application into 3D collaborative environment.

From the above, the construction scheme of 3D symbiotic environment proposed in this paper has solved the issues to construct an intuitive collaborative work environment.

6 Conclusion

Aiming to bridge the gaps between the real space and virtual spaces, and construct an intuitive collaborative work environment, we proposed the construction scheme of 3D symbiotic environment which is collaborative work environment based on Symbiotic Computing. In this paper, we presented fundamental technologies for 3D symbiotic environment. In addition, we show the design and implementation of the prototype system, and confirmed feasibility of 3D symbiotic environment with experimental results of the prototype system.

In our future work, we will improve UI description of agent on symbiotic space. UI description of the prototype system is almost similar with traditional 2D based UI, thus it's integration to 3D interaction based collaborative work is not enough. We will investigate new UI description that agent actively carry out 3D interaction based collaborative work.

References

1. Broll, W., Lindt, I., Ohlenburg, J., Herbst, I., Wittkamper, M., Novotny, T.: An infrastructure for realizing custom-tailored augmented reality user interfaces. IEEE Transactions on Visualization and Computer Graphics 11(6), 722–733 (2005)
2. Fujita, S., Sugawara, K., Kinoshita, T., Shiratori, N.: An approach to developing human-agent symbiotic space. In: Proceedings of the 2nd Joint Conference on Knowledge-Based Software Engineering (JCKBSE 1996), March 1996, pp. 11–18 (1996)
3. Hara, H., Sugawara, K., Kinoshita, T., Uchiya, T.: Flexible distributed agent system and its application. In: Proceedings of the 5th Joint Conference of Knowledge-based Software Engineering, pp. 72–77. IOS Press, Amsterdam (2002)
4. Human Interface Technology Laboratory, the University of Washington: Artoolkit home page, http://www.hitl.washington.edu/artoolkit/
5. LG3D: Project looking glass, https://lg3d.dev.java.net/
6. Milgram, P., Kishino, F.: A taxonomy of mixed reality visual displays. IEICE Transactions on Information and Systems E77-D(12), 1321–1329 (1994)
7. Wagner, D., Pintaric, T., Ledermann, F., Schmalstieg, D.: Towards massively multi-user augmented reality on handheld devices. In: Gellersen, H.-W., Want, R., Schmidt, A. (eds.) PERVASIVE 2005. LNCS, vol. 3468, pp. 208–219. Springer, Heidelberg (2005)

A Cryptographic Algorithm Based on Hybrid Cubes

Sapiee Jamel, Tutut Herawan, and Mustafa Mat Deris

Faculty of Information Technology and Multimedia
Universiti Tun Hussein Onn Malaysia
Parit Raja, Batu Pahat 86400, Johor, Malaysia
{sapiee,mmustafa}@uthm.edu.my, tutut81@uad.ac.id

Abstract. Cryptographic algorithms are important to ensure the security of data during transmission or storage. Many algorithms have been proposed based on various transformation and manipulation of data. One of which is using magic cube. However, the existing approaches are based on a transformation of magic cube's face values. In this paper, we propose a new cryptographic algorithm based on combinations of hybrid magic cubes which are generated from a magic square and two orthogonal Latin squares. Using two random functions, i.e., random selection of thirteen magic cubes and random key selection from layers of hybrid, the generated chipertexts are free from any predicted pattern which might be used by cryptanalyst to decipher the original message.

Keywords: Cryptographic algorithms, Magic Cubes, Hybrid Cubes.

1 Introduction

Cryptography is the art and science of keeping message or data secured from any unintended users or recipients. In cryptography, the processes of encryption and decryption of data and key generation are generally based on mathematical modeling. Using this method, cryptographic designers can define, describe and show that a cryptographic model proposed by them is mathematically correct. The importance of cryptography is apparent with the advent of complex network technologies (such as Internet) where data are no longer confined by physical boundaries [1]. Unfortunately, a totally secure cryptographic algorithms are difficult to build due to the existence of challenges from cryptanalysts whose objectives are to find ways to defeat any known cryptographic algorithms. Furthermore, every cryptographic algorithm must pass the test of time and general acceptance by cryptographic communities as shown in the selection of Advanced Encryption Standard (AES) [2]. Many cryptographic algorithms have been proposed including the works of [3, 4]. In [3], Daemen *et al*. proposed a cryptographic algorithm which uses Maximum Distance Separable (MDS) matrices as part of it diffusion element which is based on the earlier work of [5]. Schneier *et al*. [4] on the other hand, used combination of MDS and Pseudo-Hadamard Transformation (PHT) as the diffusion function. Wu *et al.* used matrix scrambling which is based on shifting and exchanging rule of bi-column bi-row circular queue [6]. However, all proposed algorithms are still using a two dimensional approach.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 175–187, 2010.

Another approach for a cryptographic algorithm is based on a magic cube. Magic cube puzzle is firstly proposed by Erno Kubik in 1974 which has a mathematical equivalent of magic cube where the sum of the numbers on each row, column and diagonal are the same [7]. In a magic cube game, cube surfaces are used to generate six different combinations with different surface colors. An operation such as shifting and rotating surfaces become keys to get the original cube. In 1998, Trenkler proposed a method for constructing a magic cube using magic square and two orthogonal Latin squares [8, 9]. However, the sum of numbers along main diagonal elements of the cube is not equal with that row and column. To improve the earlier method, he proposed a construction of a magic cube using a new method using different formula instead of using magic square and two orthogonal Latin squares [10]. The result stated that the sum of numbers along main diagonal elements of the cube is equal with that row and column.

An adoption of a magic cubes transformation as part of design element of cryptographic algorithm appears in several image encryption algorithms. Shen *et al.* proposed a color image encryption algorithm based on magic cube transformation and modular arithmetic operation [11]. Zhang *et al.* [12] proposed magic cube transformation for image scrambling. These algorithms use combination of magic cube games formulation and chaotic theory as part of diffusion element for enhancing complexity of the overall algorithm.

In this paper, we propose a new cryptographic algorithm using magic cubes of order 4, because the layers of a magic cube of order 4, i.e., 4×4 sized matrices are being used as basis for message block of 128-bit cryptographic algorithm.

Since the number of magic cubes of order 4 is not known, thus we use the construction of magic cubes of [8, 9], instead of that in [10]. It is based on [13], that Suzuki described there are 880 different magic squares of order 4 can be defined using combination of positive integers in $\{1,\cdots,4^2\}$. We use these magic squares to produce 880 different "magic cubes" of order 4 using two fix orthogonal Latin squares.

The rest of the paper is organized as follows: Section 2 describes preliminaries used in this paper. Section 3 outlines the proposed cryptographic algorithm which consists of key schedule algorithm, encryption algorithm and decryption algorithm. Section 4 discusses the conclusion and future work of this research.

2 Preliminaries

We use the following definitions when describing the construction of the cryptographic algorithm.

2.1 Quasi Group

Definition 1. *(See* [14]*). Let G be a nonempty set with one binary operation* $(*)$*. Then G is said to be a groupoid and is denoted* $(G,*)$.

Definition 2. *(See* [14]*). A groupoid* $(G,*)$ *is said to be a quasigroup (i.e. algebra with one binary operation* $(*)$ *on the set G) satisfying the law:*

$$(\forall u, v \in G)(\exists\, !x, y \in G)(u * x = v \wedge y * u = v).$$

This implies:

a. $x * y = x * z \vee y * x = z * x \Rightarrow y = z$

b. The equations $a * x = b, y * a = b$ have an unique solution x, y for each $a, b \in G$.

However, in general, the operation $(*)$ is neither a commutative nor an associative operation. Quasigroups are equivalent to the more familiar Latin squares. The multiplication table of a quasigroup of order *n* is a Latin square of order *n*, and conversely, every Latin square of order *n* is the multiplication table of a quasigroup of order *n*.

2.2 Latin Square

A Latin square of order *n* is an $n \times n$ matrix where each element can occur exactly once in each row and column.

Definition 3. *A Latin square of order n, denoted as*

$$R_n = [r(i, j) : 1 \le i, j \le n]$$

is a two dimensional $(n \times n)$ *matrix such that every row and every column is a permutation of the set of natural number* $\{1, \cdots, n\}$.

Thus, a Latin square is a square array in which each row and column consists of the same set of entries without repetition.

Definition 4. *Two Latin squares,* $R_n = [r(i, j)]$ *and* $S_n = [s(i, j)]$ *are said to be orthogonal if whenever* $i, i', j, j' \in \{1, \ldots, n\}$ *are such that*

$$[r(i, j)] = [r(i', j')] \text{ and } [s(i, j)] = [s(i', j')],$$

then we must have

$$i = i' \text{ and } j = j'.$$

Thus, two Latin Squares $R_n = [r(i, j)]$ and $S_n = [s(i, j)]$ order *n* are said to be orthogonal if and only if the n^2 pair $r(i, j)$ and $s(i, j)$ are all different.

2.3 Magic Square

Definition 5. *A magic square of order n, denoted as*

$$M_n = [m(i, j) : 1 \le i, j \le n]$$

is a two dimensional $n \times n$ *matrix (square table) containing the natural numbers* $1, \cdots, n^2$ *in some order such that the sum of the number along every row, column and main diagonal is a fixed constant of*

$$\frac{n\left(n^2+1\right)}{2}.$$

A "magic square" can be generated from two orthogonal Latin squares as stated in [8,9].

2.4 Magic Cube

Definition 5. (See [8]). *A magic cube of order n, denoted as*

$$Q_n = \left[q(i,j,k) : 1 \le i,j,k \le n\right]$$

is a three dimensional $n \times n \times n$ *matrix (cubical table) containing the natural numbers* $1,\cdots,n^3$ *in some order, such that*

$$\sum_{i=1,\cdots,n} q(i,j,k) = \sum_{j=1,\cdots,n} q(i,j,k) = \sum_{k=1,\cdots,n} q(i,j,k) = \frac{n\left(n^3+1\right)}{2},$$

for all $i,j,k = 1,2,3,\cdots,n$.

The triple of numbers (i,j,k) is called the coordinates of the element $q(i,j,k)$. The existence of magic cubes is given in the following theorem.

Theorem 1. (See [8]). *For every natural number* $n \neq 2$, *there exist a magic cube of order n.*

The detail proof can be found in [8]. According to [8, 9], a magic cube can be constructed using two orthogonal Latin squares.

Let $R_n = \left[r(i,j) : 1 \le i,j \le n\right]$ and $S_n = \left[s(i,j) : 1 \le i,j \le n\right]$ be two orthogonal Latin squares of order *n* and let $M_n = \left[m(i,j) : 1 \le i,j \le n\right]$ be a magic square of order *n*. A magic cube $Q_n = \left[q(i,j,k) : 1 \le i,j,k \le n\right]$ is defined using the following formula

$$q(i,j,k) = \left(s\left(i, r(j,k)-1\right)\right)n^2 + m\left(i, s(j,k)\right),$$

for all $i,j,k = 1,2,3,\cdots,n$.

The process of construction can be depicted in Figure 1.

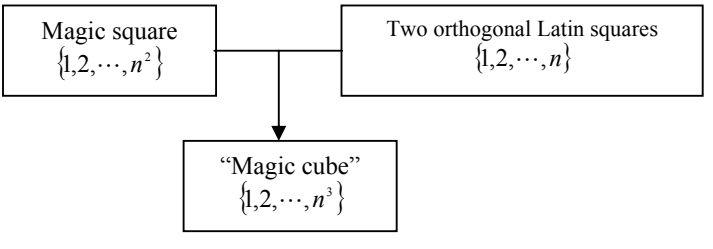


Fig. 1. Process of constructing a "magic cube"

The three dimensional coordinates for magic cube of order 4 can be depicted in Figure 2.

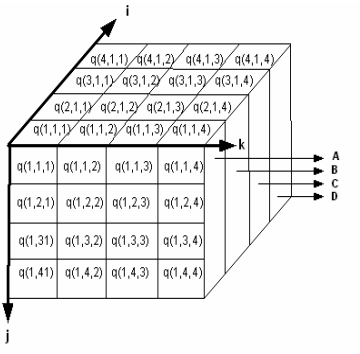


Fig. 2. Coordinates of magic cube of order 4

The "magic cubes" of order 4 generated using 880 magic squares of order 4 are non standard in the sense that the sum of numbers in main diagonal are not equal with that of row and column. Four layers, A, B, C and D, as shown in Figure 2 are used as the foundation to build the encryption keys algorithm. Each layer forms four 4×4 matrices which become the main structure in our algorithm formulation.

3 A Cryptographic Algorithm Based on Hybrid Cubes

3.1 The Model

The model of cryptographic algorithm presented in this paper is based on hybrid layers of 880 "magic cubes". We select two layers from two different "magic cubes". Then we apply inner matrix multiplication to these layers. This process is repeated with three other layers to obtain a *hybrid cube*. In total, there are 879 hybrid cubes which can be used in our algorithm. We show that all layers inside the hybrid cubes are invertible. The pair of cubes and its associated "inverse cube" is used as the building block for our key schedule construction. Since the entries of a magic cube of order 4 is a number in $\{1,\cdots,4^3\}$, then the total of hybrid cubes for key construction are 832 of 880. It means there are 13 groups containing 64 hybrid cubes. To sort the 832 pairs of hybrid cubes and its associated inverse, we use indexing method. We randomly select 13 from 880 generated "magic cubes" to become the index for sorting. From first 64 hybrid cubes, we sort using entries in a layer selected from the first of 13 "magic cubes". The second cube is used to sort the next 64 magic cubes. This process is continued until the last 64 hybrids cubes. Thus, we have 832 sorted hybrid cubes with associated inverse. In this approach, key is a layer of a sorted hybrid which is used for encryption, meanwhile the associated inverse is used for decryption. Key 1 can be selected from one of all layers in hybrid one. Clearly, our propose model is different with the previous work of [11, 12]. Additionally, since we

employ 4 layers in magic cubes i.e., we can split a magic cube of order 4 into 4 different layers using fix coordinate instead of its surfaces (6 surfaces), then we have many possibility to implement different version based on different coordinate. Hence, the complexity of the proposed model can be ensured. The notion of hybrid cubes proposed here is given in the following sub-section.

3.2 Hybrid Cubes

Hybrid cube is formed using inner matrix multiplication of layers between two "magic cubes". For example, hybrid 1 is based on inner matrix multiplication of layer in the same coordinate $(i = 1,2,3,4)$ of "magic cube" 1 and layer $(i = 1,2,3,4)$ of "magic cube" 2. Hybrid 2 is based on matrix multiplication of cube 2 and 3, and so on.

Definition 7. *Let "$\times$" be an inner matrix multiplication. A hybrid cube (of order 4) denoted by* $H_{i,j}$, $i \in \{1,\ldots,879\}$ *and* $j \in \{1,2,3,4\}$ *is defined as*

$$H_{i,j} = C_{i,j} \times C_{i+1,j},$$

where $C_{i,j}$ *is the* j^{th}*-layer of* i^{th}*-magic cube.*

Hybridization of magic cubes can be depicted in Figure 3.

$$\underbrace{\begin{bmatrix} a_{111} & a_{112} & a_{113} & a_{114} \\ a_{121} & a_{122} & a_{123} & a_{124} \\ a_{131} & a_{132} & a_{133} & a_{134} \\ a_{141} & a_{142} & a_{143} & a_{144} \end{bmatrix}}_{\text{Layer } i=1 \text{ of MC1}} \times \underbrace{\begin{bmatrix} b_{111} & b_{112} & b_{113} & b_{114} \\ b_{121} & b_{122} & b_{123} & b_{124} \\ b_{131} & b_{132} & b_{133} & b_{134} \\ b_{141} & b_{142} & b_{143} & b_{144} \end{bmatrix}}_{\text{Layer } i=1 \text{ of MC2}} = \underbrace{\begin{bmatrix} ab_{111} & ab_{112} & ab_{113} & ab_{114} \\ ab_{121} & ab_{122} & ab_{123} & ab_{124} \\ ab_{131} & ab_{132} & ab_{133} & ab_{134} \\ ab_{141} & ab_{142} & ab_{143} & ab_{144} \end{bmatrix}}_{\text{Layer } i=1 \text{ of HC1}}$$

$$\vdots$$

$$\underbrace{\begin{bmatrix} a_{411} & a_{412} & a_{413} & a_{414} \\ a_{421} & a_{422} & a_{423} & a_{424} \\ a_{431} & a_{432} & a_{433} & a_{434} \\ a_{441} & a_{442} & a_{443} & a_{444} \end{bmatrix}}_{\text{Layer } i=4 \text{ of MC1}} \times \underbrace{\begin{bmatrix} b_{411} & b_{412} & b_{413} & b_{414} \\ b_{421} & b_{422} & b_{423} & b_{424} \\ b_{431} & b_{432} & b_{433} & b_{434} \\ b_{441} & b_{442} & b_{443} & b_{444} \end{bmatrix}}_{\text{Layer } i=4 \text{ of MC2}} = \underbrace{\begin{bmatrix} ab_{411} & ab_{412} & ab_{413} & ab_{414} \\ ab_{421} & ab_{422} & ab_{423} & ab_{424} \\ ab_{431} & ab_{432} & ab_{433} & ab_{434} \\ ab_{441} & ab_{442} & ab_{443} & ab_{444} \end{bmatrix}}_{\text{Layer } i=4 \text{ of HC1}}$$

Fig. 3. Hybridization of magic cubes

3.3 The Proposed Algorithms

The proposed algorithms consist of key schedule, encryption and decryption algorithms.

3.3.1 Key Schedule Algorithm. There are 5 steps involved in the construction of key schedule algorithm using hybrid cubes. Figure 4 shows the steps for finding the key schedule.

Input : Message (4 matrices of order 4)
Output: Ciphertext (4 matrices of order 4)
Steps:

- Step 1
  Messages are formatted into four 2D matrices of 4×4 of size 16 bytes integers (Extended ASCII Codes).

- Step 2
  Message 1 is mixed with Initial Matrix (IM) which is generated from Key Schedule Algorithm to create Message 1′. This message is then mixed with key 1 to form ciphertext 1.

- Step 3
  Mixed Message 1′ with Message 2 to form Message 2′. This message is added with Key 2 to form Ciphertext 2.

- Step 4
  Repeat Step 3 with Message 3 and Message 4 to generate Ciphertext 3 and 4.

Fig. 4. Encryption Algorithm

3.3.2 Encryption Algorithm. Message size for the encryption algorithm is 64 bytes of decimal ASCII characters. Steps for the encryption algorithm are depicted in Figure 5.

3.3.3 Decryption Algorithm. The decryption algorithm is performing by applying reverse operation of encryption algorithm using appropriate decryption keys as in Figure 6.

We elaborate the proposed encryption and key schedule algorithms through a simple example as follow.

3.4 Example

3.4.1 Hybrid Cube

Based on these proposed algorithms, we give an example for performing encryption and decryption of messages.

Let

$$\mathcal{M} = \{M_i : 1 \le i \le 880\}, \tag{1}$$

be a collection of all 880 magic squares of order 4 as in [13], then we choose one as given below

$$M_i = \begin{bmatrix} 1 & 2 & 15 & 16 \\ 13 & 14 & 3 & 4 \\ 12 & 7 & 10 & 5 \\ 8 & 11 & 6 & 9 \end{bmatrix}$$

Input : Two fixed orthogonal Latin square and 880 magic square of order 4
Output: Encryption and decryption keys of 4×4 matrix.
Steps:

- Step 1
  Generate 880 "magic cubes" using two orthogonal Latin squares and 880 magic squares. These cubes are non-standard magic cubes (i.e., the sum of all numbers along main diagonal is not equal with that in rows and columns).
- Step 2
  The 880 cubes are used to generate 879 hybrid cubes using inner matrix multiplication in each layer between two adjacent cubes. The entries of a generated hybrid cubes is belong to the set $\{1,2,\ldots,4096\}$.
- Step 3
  Generate inverse for all the layers of the hybrid cubes which are used as the decryption keys.
- Step 4
  Select randomly 13 cubes from 880 magic cubes as in step 1. Each cube entries are used to sort 64 hybrids. 832 are then selected from 880 hybrid cubes. These hybrid cubes are then group into 13 subgroup of 64 hybrid cubes (13 * 64 entries = 832). Repeat this process until all 832 hybrids are sorted based on the entries of 13 cubes.
- Step 5
  Select at random one layer (4×4) matrix from hybrid one as the encryption key. The second key is selected from the second hybrid using similar technique. Generate the number of keys required based on message size.
  Choose key at random for the Initial Matrix (IM).

This process is repeated until the numbers of keys required by the encryption algorithm.

Fig. 5. Key Schedule Algorithm

The two orthogonal Latin squares are given as follows

$$LS_1=\begin{bmatrix}1&2&3&4\\2&1&4&3\\3&4&1&2\\4&3&2&1\end{bmatrix} \text{ and } LS_2=\begin{bmatrix}1&2&3&4\\3&4&1&2\\4&3&2&1\\2&1&4&3\end{bmatrix}. \tag{2}$$

```
Input  : Ciphertext
Output : Original message
Steps:
 • Step 1
   Ciphertext 1 to ciphertext 4 is multiply with
   decryption key 1 to 4 to produce message1' to
   message4'.

 • Step 2
   Message1' is  deducted with IM to obtain the
   original message 1. Message 2  is obtained by
   subtracting Message2' with Message1'.
   Message 3 and 4  are obtained by subtracting
   Message3' with Message 2' and Message3'
   accordingly.
```

Fig. 6. Decryption Algorithm

According to [8], we obtain a "magic cube" with layers in the *i*-coordinate as

$$Q_{i=1}=\begin{bmatrix}10&38&63&19\\28&56&33&13\\39&11&18&62\\53&25&16&36\end{bmatrix},\ Q_{i=2}=\begin{bmatrix}21&57&48&4\\7&43&50&30\\60&24&1&45\\42&6&31&51\end{bmatrix}$$

$$Q_{i=3}=\begin{bmatrix}44&8&17&61\\58&22&15&35\\5&41&64&20\\23&59&34&14\end{bmatrix},\ Q_{i=4}=\begin{bmatrix}55&27&2&46\\37&9&32&52\\26&54&47&3\\12&40&49&29\end{bmatrix}. \tag{3}$$

In total, based on (1) and (2) there are 880 "magic cubes".

For constructing a hybrid cube, we need another different magic cube as in (3) above. We can select a magic square from (1) to generate another "magic cube" as shown below. Let, the second magic cube with layers in the *i*-coordinate are given as follow.

$$R_{i=1}=\begin{bmatrix}2&46&59&23\\32&52&41&5\\47&3&22&58\\49&29&8&44\end{bmatrix},\ R_{i=2}=\begin{bmatrix}17&61&40&12\\15&35&54&26\\64&20&9&37\\34&14&27&55\end{bmatrix}$$

$$R_{i=3}=\begin{bmatrix}48&4&25&53\\50&30&11&39\\1&45&56&28\\31&51&38&10\end{bmatrix},\ R_{i=4}=\begin{bmatrix}63&19&6&42\\33&13&24&60\\18&62&43&7\\16&36&57&21\end{bmatrix}. \tag{4}$$

Based on Definition 7, from (3) and (4), we get a hybrid cube

$$H_{1,1}=\begin{bmatrix}20 & 1748 & 3717 & 437\\ 896 & 2912 & 1353 & 65\\ 1833 & 33 & 396 & 3596\\ 2597 & 725 & 128 & 1584\end{bmatrix},\ H_{1,2}=\begin{bmatrix}357 & 3477 & 1920 & 48\\ 105 & 1505 & 2700 & 780\\ 3840 & 480 & 9 & 1665\\ 1428 & 84 & 837 & 2805\end{bmatrix}$$
$$H_{1,3}=\begin{bmatrix}2112 & 32 & 425 & 3233\\ 2900 & 660 & 165 & 1365\\ 5 & 1845 & 3584 & 560\\ 713 & 3009 & 1292 & 140\end{bmatrix},H_{1,4}=\begin{bmatrix}3465 & 513 & 12 & 1932\\ 1221 & 117 & 768 & 3120\\ 468 & 3348 & 2021 & 21\\ 192 & 1440 & 2793 & 609\end{bmatrix} \quad (5)$$

In total, we have 879 different hybrid cubes.

For selection of encryption key, we select randomly 13 cubes from 880 magic cubes as in (3). Each cube entries are used to sort 64 hybrid cubes. After that, 832 are then selected from 880 hybrid cubes. These hybrid cubes are then group into 13 subgroup of 64 hybrid cubes (13 * 64 entries = 832). Repeat this process until all 832 hybrids are sorted based on the entries of 13 cubes.

For example, the first magic cube selected from 880 magic cubes is the 40th magic cube. With the layer of $i=1$ is given as follows

$$Q_{40,1}=\begin{bmatrix}5 & 41 & 64 & 20\\ 28 & 54 & 35 & 13\\ 42 & 8 & 17 & 63\\ 55 & 27 & 14 & 34\end{bmatrix}. \quad (6)$$

Since $q(1,1,1)=5$. Therefore we can sort the first group 64 hybrid cubes, where the 5th hybrid cube became the first sorted hybrid cube.

Based on the first sorted hybrid cube, we select the first encryption key as follow.

$$\text{Key1}=H_{5,3}=\begin{bmatrix}1776 & 16 & 625 & 3392\\ 2900 & 570 & 66 & 1833\\ 12 & 2025 & 3136 & 476\\ 713 & 3162 & 1634 & 20\end{bmatrix},$$

The first encryption key is layer $i=3$ of the first sorted hybrid cube. The remainder encryption keys are based on $q(1,1,j)$ as in (6), where $j=2,3,4$. Therefore, for $i=2$, $i=1$ and $i=4$, we have the following encryption keys

$$\text{Key2}=H_{41,2}=\begin{bmatrix}494 & 3969 & 1444 & 30\\ 168 & 1620 & 3192 & 391\\ 3392 & 324 & 121 & 1776\\ 1287 & 52 & 600 & 3720\end{bmatrix},$$

$$\text{Key3} = H_{64,1} = \begin{bmatrix} 176 & 1369 & 3224 & 500 \\ 442 & 3528 & 1386 & 120 \\ 1330 & 144 & 551 & 3294 \\ 3410 & 450 & 112 & 1462 \end{bmatrix},$$

$$\text{Key4} = H_{20,4} = \begin{bmatrix} 3465 & 513 & 12 & 1932 \\ 1728 & 81 & 640 & 2809 \\ 468 & 3348 & 2021 & 21 \\ 13 & 1600 & 2989 & 784 \end{bmatrix},$$

respectively.

In encryption process, we use Initial Matrix (IM) for mixing the first message. We select one layer of hybrid at random and let this layer become Initial Matrix (IM). Let, say we have Hybrid No. 111 and get layer 4 as IM.

$$\text{IM} = H_{111,4} = \begin{bmatrix} 3078 & 930 & 4 & 1716 \\ 1591 & 4 & 1024 & 3127 \\ 644 & 3906 & 1188 & 54 \\ 80 & 1225 & 3721 & 624 \end{bmatrix}$$

Using the following message (MS_i), for example

$$M_1 = \begin{bmatrix} 67 & 114 & 121 & 112 \\ 116 & 111 & 103 & 114 \\ 97 & 112 & 104 & 121 \\ 32 & 105 & 115 & 32 \end{bmatrix}, \; M_2 = \begin{bmatrix} 105 & 110 & 116 & 101 \\ 114 & 101 & 115 & 116 \\ 105 & 110 & 103 & 32 \\ 97 & 110 & 100 & 32 \end{bmatrix},$$

$$M_3 = \begin{bmatrix} 102 & 117 & 110 & 46 \\ 69 & 118 & 101 & 114 \\ 121 & 98 & 111 & 100 \\ 121 & 32 & 99 & 97 \end{bmatrix}, \; M_4 = \begin{bmatrix} 110 & 32 & 100 & 111 \\ 32 & 105 & 116 & 44 \\ 32 & 108 & 101 & 116 \\ 32 & 116 & 114 & 121 \end{bmatrix}.$$

The ciphertext can be obtained using the procedure as in Figure 7. From the previous messages, encryption keys and IM, then we will get the corresponding ciphertext (C_i).

$$C_1 = \begin{bmatrix} 9917984 & 6678661 & 5413481 & 12677552 \\ 5689489 & 12623079 & 9904531 & 6602211 \\ 13108495 & 5471766 & 5065975 & 10496958 \\ 4569672 & 10602064 & 13259380 & 4656850 \end{bmatrix},$$

$$C_2 = \begin{bmatrix} 5099476 & 14947122 & 9563129 & 8152610 \\ 9469185 & 8154441 & 5483478 & 14832918 \\ 6109677 & 10507878 & 14691195 & 4886988 \\ 14581543 & 4473361 & 4473361 & 10119006 \end{bmatrix},$$

$$C_3 = \begin{bmatrix} 8567858 & 9999925 & 12880706 & 5925554 \\ 14068440 & 5516872 & 7828899 & 10519596 \\ 5032572 & 16352239 & 9740610 & 6348384 \\ 8627050 & 6831779 & 5472220 & 14742972 \end{bmatrix},$$

$$C_3 = \begin{bmatrix} 14369655 & 6790917 & 8207296 & 11985782 \\ 8296947 & 11566413 & 13725186 & 7766372 \\ 11588559 & 6870255 & 7222383 & 14281655 \\ 6037434 & 15607152 & 12037791 & 6119813 \end{bmatrix},$$

respectively.

The original message can be obtained using the following decryption keys (D_i).

$$D_1 = \begin{bmatrix} -3.557729e-004 & 6.159956e-004 & 1.723832e-004 & -2.196398e-004 \\ 1.751067e-004 & -2.456201e-004 & -3.258550e-004 & 5.683296e-004 \\ -1.899183e-004 & 2.109244e-004 & 5.576952e-004 & -3.942192e-004 \\ 5.152564e-004 & -3.602317e-004 & -1.914795e-004 & 1.849570e-004 \end{bmatrix},$$

$$D_2 = \begin{bmatrix} -4.376955e-005 & 3.954779e-005 & 3.671831e-004 & -1.791041e-004 \\ 3.163416e-004 & -1.483222e-004 & -5.333288e-005 & 3.850079e-005 \\ -1.627748e-004 & 3.957183e-004 & 2.367933e-005 & -5.158524e-005 \\ 3.697488e-005 & -7.543447e-005 & -1.301072e-004 & 3.385635e-004 \end{bmatrix},$$

$$D_3 = \begin{bmatrix} -8.775146e-005 & 7.124091e-005 & 4.779873e-004 & -2.945647e-004 \\ 3.723660e-004 & -1.915392e-004 & -9.453425e-005 & 7.636747e-005 \\ -1.782215e-004 & 3.519387e-004 & 6.928347e-005 & -7.928856e-005 \\ 6.504418e-005 & -7.563081e-005 & -2.751680e-004 & 4.513776e-004 \end{bmatrix},$$

$$D_4 = \begin{bmatrix} 5.113212e-004 & -4.044562e-004 & -1.609877e-004 & 1.933999e-004 \\ -1.827121e-004 & 2.315203e-004 & 5.088421e-004 & -3.928907e-004 \\ 1.879346e-004 & -2.967962e-004 & -3.124828e-004 & 6.086391e-004 \\ -3.520974e-004 & 6.657518e-004 & 1.555569e-004 & -2.463153e-004 \end{bmatrix}.$$

The example shows that combination of “magic cubes” layers can be used to generate hybrid cubes and random selection of its layers form good encryption and decryption keys.

4 Conclusion and Future Work

In this paper, we have shown that layers of hybrid cube of order 4 can be used as building block for the development of cryptographic algorithm. In this algorithm, data

structure which consists of hybrid layers and its associated inverses become the encryption and decryption keys. The introduction of two random functions, i.e., random selection of thirteen magic cubes and random key selection from layers of hybrid avoid any predicted pattern which might be used by cryptanalyst to decipher the original message. The result of this research can be extended to develop hybrid cubes of order 8, 16, 32 and 64 based on combination of "magic cubes" order 4 which can form the foundation of new cryptographic algorithm with various matrices sizes.

Acknowledgement

The authors would like to thank Universiti Tun Hussein Onn Malaysia for supporting this research.

References

[1] Schneier, B.: Keynote Speaker. In: Hack in the Box Security Conference (HITBC), Kuala Lumpur, Malaysia (2006)
[2] National Institute of Standards(NIST): FIPS Pub 197: Advanced Encryption Standard AES (2001), http://csrc.nist.gov/
[3] Daemen, J., Rijmen, V.: The Design of Rijndael: AES – The Advanced Encryption Standard. Springer, Heidelberg (2002)
[4] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N.: The Twofish Encryption Algorithm. John Wiley and Sons, New York (1999)
[5] Vaudenay, S.: On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 286–297. Springer, Heidelberg (1995)
[6] Wu, S., Zhang, Y., Jing, X.: A Novel Encryption Algorithm based on Shifting and Exchanging Rule of Bi-Column Bi-row Circular Queue. In: International Conference on Computer Science and Software Engineerin. IEEE, Los Alamitos (2005)
[7] Wikipedia Web Site, http://en.wikipedia.org/wiki/Magic_cube
[8] Trenkler, M.: Magic Cubes. The Mathematical Gazeete 82, 56–61 (1998)
[9] Trenkler, M.: A Construction of Magic Cubes. The Mathematical Gazeete, 36–41 (2000)
[10] Trenkler, M.: An Algorithm for making Magic Cubes. The ΠME Journal 12(2), 105–106 (2005)
[11] Shen, J., Jin, X., Zhou, C.: A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation. In: Ho, Y.-S., Kim, H.-J. (eds.) PCM 2005. LNCS, vol. 3768, pp. 270–280. Springer, Heidelberg (2005)
[12] Zhang, L., Shiming, J., Xie, Y., Yuan, Q., Wan, Y., Bao, G.: Principle of Image Encrypting Algorithm Based on Magic Cube Transformation. In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) CIS 2005. LNCS (LNAI), vol. 3802, pp. 977–982. Springer, Heidelberg (2005)
[13] Heinz H.: Magic Squares. Magic Stars & Other Patterns, http://www.geocities.com/~harveyh/
[14] Snasel, Abraham, A., Dvorsky, J., Kromer, P., Platos, J.: Hash Functions Based on Large Quasigroups. In: Allen, G., Nabrzyski, J., Seidel, E., van Albada, G.D., Dongarra, J., Sloot, P.M.A. (eds.) ICCS 2009. LNCS, vol. 5544, pp. 521–529. Springer, Heidelberg (2009)

Java Implementation for Pairing-Based Cryptosystems

Syh-Yuan Tan[1], Swee-Huay Heng[1], and Bok-Min Goi[2]

[1] Faculty of Information Science and Technology, Multimedia University
Melaka, Malaysia
{sytan,shheng}@mmu.edu.my
[2] Faculty of Engineering and Science, Tunku Abdul Rahman University
Kuala Lumpur, Malaysia
goibm@utar.edu.my

Abstract. We present a Java implementation for Tate pairing over the supersingular curve $y^2 = x^3 + x$ in $\mathbb{F}_p$. We show some available optimisations for group operations by manipulating the mathematical equations. Besides, we also show that it is easy to hash a string into a point for our chosen parameters. A variant of Java's BigInteger data type, namely CpxBigInteger is created to serve equation with complex number and the Java data types are constructed: Curve, Point and Line based on CpxBigInteger. Using these data types and J2SE JDK 1.6.0_02, we implement BLS identity-based identification (IBI) scheme, which is the first rigorously defined pairing-based IBI scheme. The timings show that the Tate pairing took only 133.12 milliseconds.

Keywords: Java, pairing-based cryptosystem, elliptic curve cryptosystem.

1 Introduction

A pairing or a bilinear map is a function:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$$

where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ are groups of same prime order. The function maps a pair of points, P, Q of elliptic curve, E to an element of the multiplicative group of a finite field [3]. Pairings were initially introduced to break elliptic curve cryptosystems (ECC) due to its useful properties:

1. Bilinearlity. $e(aP, bQ) = e(P, Q)^{ab}$ for all $a, b \in \mathbb{Z}_p$.
2. Non-degeneracy. $e(P, P) \neq 1$.
3. Efficiently computable.

But it was later discovered in the work of Sakai-Ohgishi-Kasahara [25] and Boneh-Franklin [7] that pairings can be used in building cryptosystems too. This leads the researchers to a new area of cryptography, namely pairing-based cryptography (PBC). PBC gave birth to some novel cryptographic applications particularly in identity-based cryptography, such as identity-based encryption [25,7,4,5,34], hierarchical identity-based encryption [6], identity-based signature [8,11,24], identity-based identification [15,16,17], identity-based authenticated key agreement [30], etc.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 188–198, 2010.

However, not much work have been reported on the implementation as pairing based cryptosystems are more complicated compared to other well-studied cryptosystems like RSA and DSA. There are a variety of elliptic curves (supersingular, non-supersingular, hyperelliptic, etc.) and pairings (Weil, Tate, Eta, Ate, etc.) which include quite an amount of parameters. Among the curves, supersingular curves are always used because of its low extension degree and simple construction. Among the pairings, Tate pairing is favored for its better performance generally. To the best of our knowledge, there are only two publicly available pairing libraries [27,19] which are in C/C++. Though some work [32,14] had implemented pairings in Java, the source code is not available.

In this paper, we present the ways of implementing Tate pairing using the Sun Java J2SE JDK 1.6.0_02, which has not yet provided pairing based cryptographic tools in their Java Cryptography Architecture (JCA) [12]. Other service providers offered elliptic curve cryptographic library but pairing functions are not included [22].

We organise the rest of the paper as follows. We describe the parameters and algorithms to be used in Section 2. Next, we show the Java implementation and its performance in Section 3. Finally, we conclude in Section 4.

2 Parameters and Algorithms

2.1 Chosen Curve

The supersingular elliptic curve used in this paper is having the form:

$$E : y^2 = x^3 + ax + b$$

with $y, x \in \mathbb{F}_p$ and $a, b \in \{0, 1\}$. Other related terms are as follows:

- $\mathbb{F}_p$ - finite field of prime characteristic p
- $E(\mathbb{F}_p)$ - the elliptic curve over $\mathbb{F}_p$
- $\#E(\mathbb{F}_p)$ - total points on $E(\mathbb{F}_p)$
- r - the subgroup order of $E(\mathbb{F}_p)$
- k - the extension degree in order to have $E(\mathbb{F}_{p^k})$
- ϕ - the distortion map of mapping point in $E(\mathbb{F}_p)$ to $E(\mathbb{F}_{p^k})$

The prime number $p \equiv 3 \bmod 4$ needs to fulfill the requirement of $r|p+1$. In order to obtain such p, we choose the prime subgroup order r, a random value l and calculate $p = (rl) - 1$. If the resulted p does not meet the requirement mentioned, it is recalculated with another random l. Throughout this paper, we use 512 bits p and 160 bits r. Therefore l will be having bit length of approximately 352 bits. r is a Solinas prime in the form of $2^{159} + 2^{\alpha} + 1$ where $1 \leq \alpha \leq 158$ for better performance particularly in the Miller algorithm while l is in the form of $2^{352} + 2^{\alpha} + 2^{\beta}$ where $1 \leq \alpha, \beta \leq 351$. The resulted prime p is then having a low Hamming weight and subsequently speeds up the modular operation.

For our chosen supersingular curve, we set $a = 1$ and $b = 0$ so that $E : y^2 = x^3 + x$ and $\#E(\mathbb{F}_p) = p + 1$. The distortion map ϕ is defined as $\phi(x, y) = (-x, yi)$ where the non quadratic residue value i is fixed such that $i = \sqrt{-1}$. The extension degree (or known as embedding degree) k is set such that $k = 2$ in $E(\mathbb{F}_{p^k})$. If r is not coprime to $\#E(\mathbb{F}_p)$ (or $r \nmid p + 1$), it is open to anomalous attack [3].

2.2 Point Addition in $E(\mathbb{F}_p)$

For simplicity, we define a point $P \in E(\mathbb{F}_p)$ using affine coordinates (x, y) instead of projective coordinates (x, y, z). There is always an infinity point $\mathcal{O} \in E(\mathbb{F}_p)$ which acts as an identity point.

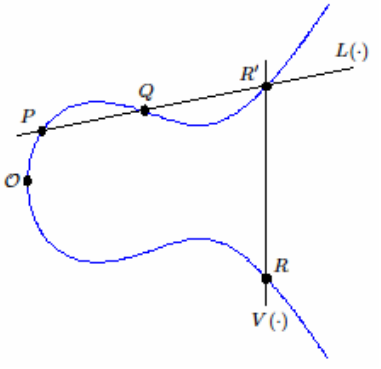


Fig. 1. $P + Q = R$

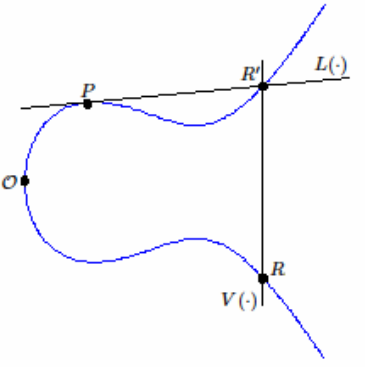


Fig. 2. $2P = R$

Consider two random points P and Q, where $P, Q \neq \mathcal{O}$ and $P \neq \pm Q$ on our chosen elliptic curve as shown in Fig. 1. If a line $L(\cdot)$ cuts through P and Q, $L(\cdot)$ will intercept the curve on a point R'. Then if we draw $V(\cdot)$, a vertical line on R', we will get another point interception on the curve, which is $-R' = R$. This process is defined as point addition on elliptic curve in $\mathbb{F}_p$ and having the mathematical form: $P + Q = R$. There are three special cases in point addition:

1. $Q = P$. $L_{P,Q}(R)$ is a tangent line as depicted in Fig. 2.
2. $Q = -P$. $L_{P,Q}(R)$ is a vertical line which intercepts at $\mathcal{O}$ since $P + (-P) = \mathcal{O}$.
3. $Q = \mathcal{O}$. Any point added with identity point $\mathcal{O}$ will get back to itself, $P + \mathcal{O} = P$.

Let $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3)$ and $P + Q = R$, the formula of point addition is as follows:

$$x_3 = \lambda - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

Note that the group operation in elliptic curve is written as addition instead of multiplication and the exponentiation can be rewritten as scalar multiplication in elliptic curve. So let $t \leq r$ and $P \in E(\mathbb{F}_p)$:

- $tP = P + P + \cdots + P$ for t times
- $0 \cdot P = rP = \mathcal{O}$

We use Double and Add algorithm as depicted in Algorithm 1 for the point scalar multiplication.

Algorithm 1. Double and Add

Require: m, P
Ensure: $Z = mP$
1: $Z \leftarrow P$
2: **for all** $i \leftarrow (\lg(m)) - 2$ to 0 **do**
3: $Z \leftarrow 2Z$
4: **if** i is 1 **then**
5: $Z \leftarrow Z + P$
6: **end if**
7: **end for**
8: **return** Z

2.3 Point Addition in $E(\mathbb{F}_{p^2})$

For points lie in the extension field $E(\mathbb{F}_{p^2})$, their coordinates are in the form of $(-x, yi)$ where $i = \sqrt{-1}$. For J2SE6 has no predefined function for complex number in BigInteger, we create a new class for the complex number, namely CpxBigInteger. The addition and multiplication algorithms in $E(\mathbb{F}_p)$ can be applied here but with a little more work on i:

- Multiplication. $(a + bi)(c + di) = ac - bd + (bc + ad)i$
- Squaring. $(a + bi)^2 = a^2 - b^2 + (2ab)i$
- Inversion. $(a + bi)^{-1} = (a - bi)(a^2 + b^2)^{-1}$
- Exponentiation. Using Algorithm 1.

2.4 Torsion Point

Suppose $P \in E(\mathbb{F}_p)$ and $rP = \mathcal{O}$, P is called a r-torsion point. The set of r-torsion points in $E(\mathbb{F}_p)$ is denoted by $E(\mathbb{F}_p)[r]$.

In order to obtain a random point, we first select a random x and then solve the selected curve for y. For the chosen curve, a square root exists for half of the values $x \in \mathbb{F}_p$ [20]. If the Jacobian symbol does not return 1 for y, this means the resulted y is a non quadratic residue and a new x is selected to repeat the same process. Since $p \equiv 3 \mod 4$, the square root of y can be easily calculated by having the exponent $(p + 1)/4$ [1]. Let $n = \#E(\mathbb{F}_p)$, the full algorithm of finding a random r-torsion point is as depicted in Algorithm 2.

2.5 Extract Torsion Point

Some schemes require extraction of a point from a given string and in fact the algorithm is not hard to be implemented. The extraction algorithm is similar to Algorithm 2. The extraction algorithm replaces the random value x with the hash value from an input string (since x-coordinate lies in $\mathbb{F}_p$, SHA-512 is chosen as the hash function) and then solve the curve for y. Thus, the amendment on Algorithm 2 is to insert:

$x \leftarrow \textbf{Hash}(string)$
$y = x^3 + ax + b$

Algorithm 2. Generate Torsion Point

Require: $E(\mathbb{F}_p), r, p, n$
Ensure: $P = (x, y)$
1: **repeat**
2: **repeat**
3: $x \xleftarrow{R} \mathbb{F}_p^*$
4: $y = x^3 + ax + b$
5: **until** $y^{(p-1)/2}$ equal 1
6: $y \leftarrow y^{(p+1)/4}$
7: $c \xleftarrow{R} 0$ or 1
8: **if** c equals 0 **then**
9: $P \leftarrow (x, y)$
10: **else**
11: $P \leftarrow (x, -y)$
12: **end if**
13: $P \leftarrow (n/r)P$
14: **until** P not equal $\mathcal{O}$
15: **return** P

before line 1 and change the repeat-until loop to:

while $y^{(p-1)/2}$ not equal 1 **do**
$x \leftarrow x + 1$
$y = x^3 + ax + b$
end while

2.6 Lines

Referring to the special cases in point addition, three types of lines are involved in Tate pairing, namely linear line, tangent line and vertical line. Recall that $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ for linear line and $\lambda = \frac{3x_1^2 + a}{2y_1}$ for tangent line, we have three equations for the values of lines:

- Linear Line, $L_{P,Q}(R) = Y - \lambda X - c$
- Tangent Line, $T_P(R) = Y - \lambda X - c$
- Vertical Line, $V_P(\mathcal{O}) = X - x_1$

where $c = y_1 - \lambda x_1$ and the points $P + Q = R$ lie on the elliptic curve $y^2 = x^3 + x$. Since the equations $L_{P,Q}(\cdot), T_P(\cdot)$ and $V_P(\cdot)$ each takes as input a point that does not lie on their respective line, the resulted value will always be a non-zero value. Note that if a line's input point is in the form of $(-x, yi)$, all operations are done using CpxBigInteger.

2.7 Tate Pairing

The Tate pairing $e(P, Q)$ requires $P \in E(\mathbb{F}_p)$ while $Q \in E(\mathbb{F}_{p^k})$ for $k > 1$. For our parameters $y^2 = x^3 + x$, $p \equiv 3 \bmod 4$ and $k = 2$, the available distortion

map ϕ is: $\phi(Q(x,y)) = (-x, yi)$ [1]. Technically, Tate pairing should be viewed as $e(P, \phi(Q))$. For details of theory and variations of Tate pairing, kindly refer to [25, 1, 32, 27, 19, 28, 20].

The core algorithm of Tate pairing is Miller algorithm [21] which was initially designed for Weil pairing. With the parameters chosen, we use the modified Miller algorithm for Tate pairing from [1]:

Algorithm 3. Tate Pairing

Require: $P \in E(\mathbb{F}_p), Q \in E(\mathbb{F}_{p^2}), r, p$
Ensure: $e(P, Q)$
1: $f \leftarrow 1$
2: $Z \leftarrow P$
3: **for all** i from $(\lg r) - 2$ to 0 **do**
4: $\quad f \leftarrow f^2 \cdot T_Z(Q)$
5: $\quad Z \leftarrow 2Z$
6: $\quad$ **if** i is 1 **then**
7: $\quad\quad f \leftarrow f \cdot L_{Z,P}(Q)$
8: $\quad\quad Z \leftarrow Z + P$
9: $\quad$ **end if**
10: **end for**
11: **return** $f^{(p^2-1)/r}$

Notice that in line 7 and line 8, the same points Z and P are used. So we can reuse the calculated λ of line 7 in line 8 and save one calculation of λ.

The final exponent $(p^2 - 1)/r$ is used to standardise the coset representative $f \in \mathbb{F}^*_{p^2}$, which represents the coset $f\mathbb{F}^{*r}_{p^2}$. To simplify the calculation $f^{(p^2-1)/r} = f^{(p+1)/r \cdot (p-1)}$, we first compute $f' = f^{(p+1)/r} = a + bi$. Since $f = f'^{p-1} = (a + bi)^{p-1} = (a^p + (bi)^p)/(a + bi)$ and $p \equiv 3 \bmod 4$, this implies $i^p = -i$ and we can rewrite f as:

$$f = \frac{a^2 - b^2}{a^2 + b^2} - \frac{2abi}{a^2 + b^2}$$

3 Java Implementation

Based on the parameters and algorithms, four new Java data types were constructed. As depicted in Table 1, CpxBigInteger's constructor takes a BigInteger array and a BigInteger value p as input. The array represents the value of a and b in $a + bi$ and the presence of imaginary number i is managed using boolean data type. While the value p is the prime value p where the finite field $\mathbb{F}$ lies on.

Table 2 shows that the class Curve provides two constructors. The first generates a random supersingular curve following the way shown in Section 2.1 while the second customises the curve. Customizable constructor is always needed particularly in expanding an existing system.

The classes from Table 1 to 3 implement java.io.Serializable but not the class Line which is used during internal calculation of Tate pairing only. Serializable enables

Table 1. Class Structure: CpxBigInteger

Return	Function
CpxBigInteger	CpxBigInteger(BigInteger[] value, BigInteger p)
CpxBigInteger	multiply(CpxBigInteger cpx)
CpxBigInteger	pow(BigInteger i)
CpxBigInteger	square()
CpxBigInteger	Inverse()
boolean	equals()

Table 2. Class Structure: Curve

Return	Function
Curve	Curve()
Curve	Curve(BigInteger a, BigInteger b, BigInteger p, BigInteger n, BigInteger order)
Point	Point(BigInteger x, BigInteger y)
Point	Point(BigInteger x, boolean xi, BigInteger y, boolean yi)
Point	getTorsionPoint()
Point	ExtractTorsionPoint(String ID)
Line	NLineInit(Point P, Point Q)
Line	TLineInit(Point P)
Line	VLineInit(Point P)
CpxBigInteger	TatePairing(Point P, Point Q)

Table 3. Class Structure: Point

Return	Function
Point	Point(Curve curve, BigInteger x, boolean xi, BigInteger y, boolean yi)
Point	Add(Point Q)
Point	Multiply(BigInteger m)
Point	negate()
Point	DistortionMap()
Point	clone()
boolean	isInfinity()

Table 4. Class Structure: Line

Return	Function
Line	Line(BigInteger a, BigInteger b, BigInteger lamda, BigInteger v, BigInteger p, int type)
CpxBigInteger	ValueOn(Point R)

the class which implements it to support socket programming. This indicates that the classes CpxBigInteger, Curve and Point are ready to be used in the client-server environment.

3.1 Case Study: BLS Identity-Based Identification (BLS-IBI) Scheme

An identification scheme assures one party (through acquision of corroborative evidence) of both the identity of a second party involved, and that the second party was active at the time the evidence was created. Common applications of identification are

ATM Card, Credit Card, Identity Card, E-voting, etc. Meanwhile, identity-based cryptography is a concept formalied by Shamir in 1984 [29] where the public key is replaced by the user's public identity, which normally considered as a string (email address, name, phone numbers, etc.). The interesting part of identity-based cryptography is it needs no keys or certificates storage. This greatly reduces the complexity of public key cryptography for no data managing and searching is needed.

Combination of these two ideas gives us the identity-based identification scheme but there was no rigorous proof until the independent works of Kurosawa and Heng [15] and Bellare et al. [2]. As the first formally defined IBI (also the first formally defined pairing-based IBI) in [15], BLS-IBI is chosen for our case study and it is defined as follows:

Setup. On input 1^k, generate an additive group $\mathbb{G}$ with prime order q. Choose $P \xleftarrow{R} \mathbb{G}$ and $s \xleftarrow{R} \mathbb{Z}_q$. Let the master public key, $mpk = (P, P_{pub}, H)$ and master secret key, $msk = s$ where $P_{pub} = sP$ and $H : \{0,1\}^* \rightarrow \mathbb{G}$.

Extract. Given a public identity **ID**, compute user private key, $d = sQ$ where $Q = H(\mathbf{ID})$.

Identification Protocol. Prover ($\mathcal{P}$) interacts with verifier ($\mathcal{V}$) as follows:

1. $\mathcal{P}$ chooses $r \xleftarrow{R} \mathbb{Z}_q$, computes $U = rQ$ and sends U to $\mathcal{V}$.
2. $\mathcal{V}$ chooses $c \xleftarrow{R} \mathbb{Z}_q$ and sends c to $\mathcal{P}$.
3. $\mathcal{P}$ computes $V = (r + c)d$ and sends V to $\mathcal{V}$.
4. $\mathcal{V}$ verifies whether $e(P, V) = e(P_{pub}, U + cQ)$.

Using the parameters mentioned in Section 2.1 and set **ID** as "user@gmail.com", the group operations and BLS-IBI scheme are executed for 1000 times on Intel Pentium M 1.6 Ghz with 512MB RAM in Windows XP Professional Edition and Knoppix Live 5.11. The performance is measured in nanosecond as depicted in Table 5 and Table 6 (Cpx stands for CpxBigInteger).

3.2 Performance

Compare to 1024 bits BigInteger operations (security of 1024 bits on $\mathbb{F}_p$ in RSA/DSA is comparable to 512 bits on $E(\mathbb{F}_{p^2})$ in ECC) in Table 2 of [33], multiplication in CpxBigInteger is 17,218ns faster and inverse in CpxBigInteger is 1,157,805ns faster. The significant difference in the performance is the exponentiation operation because the exponent of pairing is only 160 bits in length.

Next, [14] showed that their scalar multiplication in $E(\mathbb{F}_{2^{163}})$ took 116.83ms while their Eta pairing in $\mathbb{F}_{3^{97}}$ took only 10.15ms using J2SE (should be JDK 1.5 by then) on Pentium M 1.73 Ghz, which is faster for almost $[(439/391) - 1] \times 100\% \approx 12\%$ [23]. However, their modular exponentiation of 1024-bit RSA took 75.07ms while it took only 44.00ms for ours, where it is faster for approximately 41%. This is probably caused by the optimisations and updates performed by Sun Java on their BigInteger's modular exponentiation function. So, for standardisation purpose, we scale their timings

Table 5. Timing (ns) of Group Operation for Pairing Library

Operation	Syntax	Windows XP		Knoppix	
		Time in $E(\mathbb{F}_p)$	**Time in $E(\mathbb{F}_p^2)$**	**Time in $E(\mathbb{F}_p)$**	**Time in $E(\mathbb{F}_p^2)$**
Curve Generation	Curve()	1,057,162,660	-	1,163,064,634	-
Torsion Point Generation	getTorsionPoint()	135,860,919	-	142,909,986	-
Extract Torsion Point	ExtractTorsionPoint(String ID)	135,891,104	-	142,750,164	-
$P = mP$	Multiply(BigInteger m)	77,814,018	77,899,109	81,549,776	81,755,921
$R = P + Q$	P.Add(Point Q)	322,836	323,276	337,839	338,839
$e(P, Q)$	TatePairing(Point P, Point Q)	-	133,119,594	-	141,406,363
Cpx Exponentiation	pow(BigInteger i)	-	8,663,367	-	9,734,870
Cpx Multiplication	multiply(CpxBigInteger cpx)	-	45,176	-	51,351
Cpx Inverse	Inverse()	-	36,572	-	36,851
RSA modular exponentiation	modPow(BigInteger pow, BigInteger mod)	44,004,150	-	46,239,373	-

Table 6. Timing (ns) of BLS-IBI

Function	Windows XP	Knoppix
	Time	**Time**
Setup	1,330,370,941	1,633,588,064
Extract	229,168,024	246,206,534
IP	679,803,438	682,738,398
Total	2,239,342,403	2,562,532,996

to 68.93ms for scalar multiplication (and 5.99ms for Eta pairing) and it is about 8.88ms faster than ours.

Referring to Table 3 in Section IV-G of the work by [22], our timing of point scalar multiplication (in 512 bits) is about the same with that of curve P-384 and approximately half of curve P-521. According to [23], the processor (Pentium 4 2.4 Ghz) used by the author is having performance of $(325/391) \times 100\% \approx 83\%$ of ours. We scale the timings by $[(0.83 \times 0.41)/1.12] \times 100\% \approx 30\%$ and we get 113.56ms for the curve P-521, which is slower around 35.75ms than ours. We omit the comparison in Linux because the timing is slower than Windows in the author's work and also ours. Thus we assume our point operations are at least as fast as those libraries mentioned [18, 9, 10, 13] by the author.

The specification used in [32] was JDK 1.4.1 and FlexiProvider on Windows XP with a $[1 - (315/391)] \times 100\% \approx 19\%$ slower Pentium M 1400 Mhz processor. We made a scale of $[(0.81 \times 0.41)/1.12] \times 100\% \approx 30\%$ on its best timing for Tate pairings and it turns out to be 436.80ms which is roughly 323.68ms slower than ours. This is because the author was not using Solinas prime and thus their pairing requires a lot more point additions in Miller algorithm as compared to ours.

4 Conclusion

We presented the procedure of computing Tate Pairing using the supersingular curve $y^2 = x^3 + x$ on $\mathbb{F}_p$ with extension degree $k = 2$, 160 bits prime order r and 512 bits

prime characteristic p. We implemented BLS-IBI scheme using our pairing library in J2SE JDK 1.6.0_02 and the results showed that the identification protocol can be completed within 0.7 second. This is acceptable for desktop applications but improvement is still a need for mobile applications. Our future works are to consider more optimisation and implement pairing-based cryptosystems on mobile devices such as Java-enabled smart card.

References

1. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–368. Springer, Heidelberg (2002)
2. Bellare, M., Namprempre, C., Neven, G.: Security proofs for identity-based identification and signature schemes. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 268–286. Springer, Heidelberg (2004)
3. Blake, I., Seroussi, G., Smart, N.P.: Advances in elliptic curve cryptography. Cambridge University Press, Cambridge (2005)
4. Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
5. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
6. Boneh, D., Boyen, X., Goh, E.J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)
7. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
8. Boneh, D., Lynn, B., Sacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001)
9. Cryptix Project, http://www.cryptix.org/
10. FlexiProvider, http://www.flexiprovider.de/
11. Hess, F.: Efficient identity based signature schemes based on pairings. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 310–324. Springer, Heidelberg (2003)
12. Java^{TM} cryptographic architecture (JCA) reference guide for Java^{TM} Platform Standard Edition 6, http://java.sun.com/javase/6/docs/technotes/guides/security/cryptocryptospec.html
13. jBorZoi 0.90, http://dragongate-technologies.com/jBorZoi/jBorZoi_0.90.zip
14. Kawahara, Y., Takagi, T., Okamoto, E.: Efficient implementation of Tate pairing on a mobile phone using Java. In: Wang, Y., Cheung, Y.-m., Liu, H. (eds.) CIS 2006. LNCS (LNAI), vol. 4456, pp. 396–405. Springer, Heidelberg (2007)
15. Kurosawa, K., Heng, S.-H.: From digital signature to ID-based identification/signature. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 248–261. Springer, Heidelberg (2004)
16. Kurosawa, K., Heng, S.-H.: Identity-based identification without random oracles. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3481, pp. 603–613. Springer, Heidelberg (2005)

17. Kurosawa, K., Heng, S.-H.: The power of identification schemes. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 364–377. Springer, Heidelberg (2006)
18. Legion of the Bouncy Castle, http://www.bouncycastle.org/
19. Lynn, B.: PBC library (2006), http://rooster.standford.edu/-ben/pbc/download.html
20. Lynn, B.: Ph.D thesis: On the implementation of pairing-based cryptosystems (2008), http://crypto.stanford.edu/pbc/thesis.pdf
21. Miller, V.: Short programs for functions on curves. Unpublished manuscript (1986), http://crypto.stanford.edu/miller/miller.pdf
22. Nightingle, J.S.: Comparative analysis of Java cryptographic libraries for public key cryptography. George Mason University: Department of Electrical and Computer Engineering, http://ece.gmu.edu/courses/ECE746/project/specs_2006/java_multiprecision.pdf
23. PassMark® Software, http://www.cpubenchmark.net/
24. Paterson, K.G.: ID-based signatures from pairings on elliptic curves. Electronic Letters 38(18), 1025–1026 (2002); IET Digital Library
25. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: SCIS 2000 (2000)
26. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
27. Scott, M.: MIRACL library (2005), http://ftp.computing.dcu.ie/pub/crypto/miracl.zip
28. Scott, M.: Computing the Tate pairing. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 293–304. Springer, Heidelberg (2005), Available from http://ftp.computing.dcu.ie/pub/crypto/miracl.zip
29. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
30. Smart, N.P.: An identity based authenticated key agreement protocol based on the Weil pairing. Electronic Letters 38(13), 630–632 (2002); IET Digital Library
31. Solinas, J.: ID-based digital signature algorithms (2003), http://www.cacr.math.uwaterloo.ca/conferences/2003/ecc2003/solinas.pdf
32. Stögbuer, M.: Diploma thesis: Efficient algorithms for pairing-based cryptosystems (2004), http://www.cdc.informatik.tu-darmstadt.de/reports/reports/KP/Marcus_Stoegbauer.diplom.pdf
33. Tan, S.-Y., Heng, S.-H., Goi, B.-M., Chin, J.-J., Moon, S.: Java implementation for identity-based identification. International Journal of Cryptology Research 1(1), 21–32 (2009)
34. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)

On Selecting Additional Predictive Models in Double Bagging Type Ensemble Method

Zaman Faisal[1,*], Mohammad Mesbah Uddin[2], and Hideo Hirose[2]

[1] Kyushu Institute of Technology
680-4 Kawazu, Iizuka, Japan
zaman@ume98.ces.kyutech.ac.jp, hirose@ces.kyutech.ac.jp
[2] Kyushu University, Fukuoka, Japan
mesbah@slrc.kyushu-u.ac.jp

Abstract. Double Bagging is a parallel ensemble method, where an additional classifier model is trained on the out-of-bag samples and then the posteriori class probabilities of this additional classifier are added with the inbag samples to train a decision tree classifier. The subsampled version of double bagging depend on two hyper parameters, subsample ratio (SSR) and an additional classifier. In this paper we have proposed an embedded cross-validation based selection technique to select one of these parameters automatically. This selection technique builds different ensemble classifier models with each of these parameter values (keeping another fixed) during the training phase of the ensemble method and finally select the one with the highest accuracy. We have used four additional classifier models, Radial Basis Support Vector Machine (RSVM), Linear Support Vector Machine (LSVM), Nearest Neighbor Classifier (5-NN and 10-NN) with five subsample ratios (SSR), 0.1, 0.2, 0.3, 0.4 and 0.5. We have reported the performance of the subsampled double bagging ensemble with these SSRs with each of these additional classifiers. In our experiments we have used UCI benchmark datasets. The results indicate that LSVM has superior performance as an additional classifiers in enhancing the predictive power of double bagging, where as with SSR 0.4 and 0.5 double bagging has better performance, than with other SSRs. We have also compared the performance of these resulting ensemble methods with Bagging, Adaboost, Double Bagging (original) and Rotation Forest. Experimental results show that the performance of the resulting subsampled double bagging ensemble is better than these ensemble methods.

Keywords: Double Bagging, Additional Classifier Model, Sub Sampling Ratio, Stable Classifier, Embedded Cross-validation.

1 Introduction

Ensemble learning is one of the main research directions in recent years, due to their potential to improve the generalization performance of the predictors. It

* Corresponding author.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 199–208, 2010.

has attracted scientists from several fields including Statistics, Machine Learning, Pattern Recognition and Knowledge Discovery [8]. Numerous theoretical and empirical studies have been published to establish the advantages of the predictor decision combination paradigm over the single (individual) predictor [14], [11]. The success of ensemble methods arises largely from the fact that they offer an appealing solution to several interesting learning problems of the past and the present, such as improving predictive performance, learning from multiple physically distributed data sources, scaling inductive algorithms to large databases and learning from concept-drifting data streams. Most popular among the ensemble creation techniques are Bagging [2], Adaboost [9,10], Random Forest [4] and Rotation Forest [15].

In standard bagging individual classifiers are trained on independent bootstrap samples that are generated with replacement from the set of labeled training samples, where as in adaboost by *resampling* the fixed training sample size and training examples resampled according to a probability distribution are used in each iteration and in each iteration, the distribution of the training data depends on the performance of the classifier trained in the previous iteration. Unlike these two ensemble methods, Hothorn and Lausen proposed, "Double Bagging" [12] and "Bundling" [13] to add the outcomes of arbitrary classifiers to the original feature set for bagging of classification trees. Double bagging is a combination of linear discriminant analysis and classification trees. As in the bootstrap method, approximately $\frac{1}{3}$ of the observations in the original training set are not part of a single bootstrap sample in bagging [3], Breiman termed the set constituted by these observations as an out-of-bag sample. In double bagging, an out-of-bag sample (OOBS) is utilized to estimate the coefficients of a linear discriminant function (LDA) and the corresponding linear discriminant variables computed for the bootstrap sample are used as additional features for training a classification tree. In this paper we have used Radial Basis Support Vector Machine (RSVM), Linear Support Vector Machine (LSVM), Nearest Neighbor Classifier (5-NN and 10-NN) as the additional classifier models. To enlarge the OOBS size we have used five small subsample ratios (SSR), from 0.1 to 0.5.

Typically, ensemble methods comprise two phases: the production of multiple predictive models and their combination. Recently researchers [5], [6] consider an additional intermediate phase that deals with the reduction of the ensemble size prior to combination. This phase is commonly called ensemble pruning, while other names include selective ensemble, ensemble thinning and ensemble selection. The main idea of this work is to completely exclude additional learning algorithms with low performance which may produce misleading results. It seems more reasonable to select an additional model that enhance the performance significantly better than others, than to use the all models. In particular, this paper proposes: a) selecting a single predictive model as the additional model in double bagging, b) select a single SSR to create the optimum training sample size for base classifiers; using an embedded cross-validation technique. We present here a method for embedding cross-validation inside ensemble selection to maximize the amount of validation data. While adding cross-validation to ensemble

selection is computationally expensive, it is valuable for domains that require the best possible performance, and for domains in which labeled data is scarce.

The paper is organised as: in Section 2, we have described about the effect of SSR on double subagging, the subsampled version of double bagging. We have also discussed about the embedded cross-validation method in that section. In Section 3, we have stated the aim and setup of the experiments; the discussion of the results is also included in that section; this is followed by the conclusion in Section 4.

2 Double Subagging

In this section we briefly discuss about Double Subagging, the subsampled version of double bagging. The effect of small subsamples on double subagging is illustrated theoretically. We have also described the cross-validation based selection method.

When a decision tree is adopted as the base learning algorithm, only splits that are parallel to the feature axes are taken into account even though the decision tree is nonparametric and can be quickly trained. Considering that other general splits such as linear ones may produce more accurate trees, a "Double Bagging" method was proposed by Hothorn and Lausen [12] to construct ensemble classifiers. In double bagging framework the out-of-bag sample is used to train an additional classifier model to integrate the outputs with the base learning model. So we see that performance of the double bagging solely depends on two factors: 1) the classes of the dataset are linearly separable so that the additional predictors are informative (or discriminative), this implicitly implies that, the additional classifier should be able to discriminate the classes of the data, 2) the size of the out-of-bag samples as to construct an additional classifier model. However, to handle real world classification problems, the base classifier should be flexible, so in this paper we have tried four different additional classifier models. In this paper we have inserted small subsamples to train the base classifier in double bagging and defining this method as, "Double Subagging". The generic framework of double subagging algorithm is showed in Fig 1.

2.1 Effect of Small Subsampling Ratios on Double Subagging

Subsampling is a popular technique for data reduction in data mining and machine learning. Many different approaches are possible and statistical bounds on worst-case error can be used to determine a worst-case subsample size. On the other hand a purely empirical method would require plotting an error curve using increasingly larger subsample sizes until a plateau in error is seen. In this paper we have used small subsamples instead of bootstrap samples to train base classifiers for Double Subagging. There is a reason to believe that the performance of the $m(= 0.5n)$-out-of-n (subsampling) bootstrapping to perform similar to

Double Subagging Algorithm:

Input:

- X: Training set of size N.
- ρ: Small subsample ratio
- C: A base classifier, here classification tree.
- C^{add}: An additional classifier model.
- B: Number of classifiers to construct.
- x: Test instance for classification.

Output: ω: Class label for x.

Generate Small Subsamples

Step 1. Extract a small subsample of size $N * \rho$ from the training set, define this as X^b.

Generate Transformed Additional Predictors

Step 2. Construct additional classifier model c^{add} using the out-of-bag sample $X^{-(b)}$, Transform the original predictors $X^{(b)}$ using each additional classifier model c^{add}. Denote these as $c^{add}(x^{(b)})$.

Bundle Original and Additional Predictors

Step 3. Construct the combined classifier C^{comb}, by *bundling* the original predictors and the transformed predictors, as $C^{comb(b)} = (x^{(b)}, c^{add}(x^{(b)})$.

Depending on how many base classifiers we want to construct, iterate steps (2) and (3); for example B bootstrap samples.

Classification:

A new observation x_{new} is classified by, "majority" vote rule using the predictions of the combined B classifiers $C((x_{new}, c^{add}(x_{new})), C^{comb(b)})$ for $b = 1, 2, ...B$.

Fig. 1. Generic Framework of Double Subagging Algorithm

n-out-of-n bootstrap. The effective size of resample in the n-out-of-n bootstrapping in terms of amount of information it contains is

$$\frac{(\sum N_i)^2}{\sum N_i^2} \approx \frac{1}{2}n$$

where N_i denotes how many times the ith data value is repeated in the subsample. In [17] authors shown that the performance of subagging of stable (linear) classifiers are conversely related with double subagging of stable classifiers regarding the size of the subsamples. The main reason for this is, with larger OOBS (smaller subsample) the additional classifier models will be trained better (the stable base classifier will not be trained well) and will produce more accurate estimates of class probability as the additional predictors for the base decision tree. But this has a disadvantage from the time complexity point of view; with large OOBS (small subsample) the additional classifier models will take more time train than smaller OOBS (larger subsample).

2.2 Double Subagging with Ensemble Selection

The double subagging has two hyper parameters, a) additional classifier model and b) small subsampling ratio (SSR). As the performance of the algorithm

depends on the choice of these two parameters [16], one should be precise in selecting the optimum SSR and additional classifier to maximize the performance of the double subagging algorithm. With SSR an additional classifier model is trained well, so we have selected five SSR ranging from 0.1 to 0.5. For the choice of additional classifier models in [16] authors preferred RSVM over other classifiers. In this paper we have selected LSVM, 5NN and 10NN with RSVM as the additional classifier. It is computationally expensive to select both the parameters simultaneously, so our idea is to fix one and select optimum value of other, for example fix the SSR to 0.3 and select the optimum additional classifier among RSVM, LSVM, 5NN and 10NN. We have used the cross-validation to perform the selection of optimum ensemble (the ensemble with optimum additional classifier). We need a hillclimbing dataset based on which the selection will be done, where as small hillclimbing set can cause overfitting [6], to maximize the amount of available data, we apply cross-validation to ensemble selection. We embed cross-validation within ensemble selection so that all of the training data can be used for the critical ensemble hillclimbing step. Conceptually, the procedure makes cross-validated models, then runs ensemble selection the usual way on a library of cross-validated base-level models.

A cross-validated model is created by training a model multiple times (here 5 times) for different folds with the *same model parameters*, here SSR or any classifier model. As in our case we have 4 classifiers and 5 SSR; for selecting additional classifier we run 4-fold cross-validation with SSR fixed, with each fold containing a double subagged ensemble with one of the additional classifiers. For each case we repeat the whole process 5 times, for each repetition, each individual model can be defined as 'siblings'; these siblings should only differ based on variance due to their different training samples. To make a prediction for a test point, a cross-validated model simply averages the predictions made by each of the models in each repetitions. The prediction for a training point (that subsequently will be used for ensemble hillclimbing), however, only comes from the individual model that did not see the point during training. In essence, the cross-validated model delegates the prediction responsibility for a point that will be used for hillclimbing to the one sibling model that is not biased for that point.

3 Experiments and Discussion of Results

In this section we have firstly stated the aim and setup of the experiments and then we have discussed the results obtained from the experiments.

3.1 Aim and Setup of the Experiments

In this paper we have proposed an embedded cross-validation method to select the double subagging ensembles with optimum additional classifiers. We conducted two sets of experiments to check the performance of the selection method on the respective ensemble. In the first experiment we compare the double subagging with selection method and without selection method which is the

combination of outputs of all the additional classifiers rather than a single classifier, it can be also defined as Subundling [18]. We also check the performance of original versions of double bagging with bundling in the same experiment. The purpose of this experiment is to check whether the selection method enhance the performance of the double subagging (and double bagging) method. In the second experiment we have compared the best performing double subagging ensemble with several most popular ensemble methods, bagging, adaboost and rotation forest. In all our experiments we have used 15 UCI [1] benchmark datasets. The dataset descriptions are given Table 1. In all the experiments we have reported average error of 15 ten-fold cross-validation results i.e., each cell in each table consists of an average value of total 150 (15×10-CV) testing.

Table 1. Description of the 15 Data used in this paper

Dataset	Objects	Classes	Features
Diabetes	768	2	8
German-credit	1000	2	20
Glass	214	7	9
Cleveland-Heart	297	5	13
Heart-Statlog	270	2	13
Ionosphere	351	2	34
Iris	150	3	4
Liver-disorder	345	2	6
Lymphography	148	4	18
Sonar	208	2	60
Vehicle	846	4	18
Vote	435	2	16
Wiscinson-breast	699	2	9
Wine	178	3	13

For all the ensemble methods we have used a full decision tree as the base classifier. The size of all ensembles is fixed to 50. We have used five subsample ratios $0.1 - 0.5$ to build the double subagging ensembles. For each ensemble method the average error rate with their corresponding average ranks are reported in the each table. The classifier with the lowest average rank for errors are marked bold and underlined. In each table for each row (dataset) the best performing ensemble method with lowest error rate is marked in bold and underlined. For each table we performed the comparison of the methods as proposed by Demšar [7], which is described below:

- First perform the Friedman test, to check the null hypothesis that all methods have equal performance.
- Then if the null hypothesis is rejected, perform the Nemenyi posthoc test to detect the methods which are not significantly different from each other.
- Perform the Wilcoxon Sign Rank test, where we compare the *best* performing classifier with all other classifiers. We select best classifier on the basis

of lowest average rank for errors. If there are several classifiers with lower average rank for errors with very small difference, then we select the one with lowest average rank for training time among them.

We have selected these two non-parametric tests because they are appropriate since they assume limited commensurability. They are safer than parametric tests since they do not assume normal distributions or homogeneity of variance. In each table we have indicated the classifiers which are not significantly different. We have notified the classifiers of the same group as, "group a". The best performing classifier is also marked with a (*) sign in each table. The Wilcoxon Sign Rank test will clarify the performance of the *best* ensembles in each table if there is no significant difference detected by the Nemenyi posthoc test. We have given the p-values of the Wilcoxon test in the last row of each table. A high p-value in a column indicates that there is not much difference between the ensemble method of that corresponding column and the best method regarding the generalization performance in that table and vice versa.

Table 2. Comparison of error rates of double subagging and subundling in benchmark datasets

Dataset	DSB10	SB10	DSB20	DSB20	DSB30	SB30	DSB40*	SB40	DSB50	SB50	DBag	Bundle
Diabetes	0.234	0.237	0.237	0.245	0.235	0.241	**0.233**	0.238	0.238	0.245	0.240	0.248
German	0.225	0.230	0.232	0.232	0.230	0.232	0.225	**0.222**	0.224	0.226	0.232	0.225
Glass	0.314	0.359	0.255	0.301	0.226	0.290	0.224	0.265	**0.207**	0.249	0.230	0.241
Heart	0.159	0.164	0.151	0.157	0.164	0.154	0.159	0.158	0.164	**0.149**	0.172	0.167
Hearts	0.161	0.162	0.161	0.163	0.161	0.163	0.163	0.167	**0.159**	0.170	0.190	0.170
Ion	0.073	0.064	0.060	0.063	**0.059**	0.064	**0.059**	0.064	0.064	0.065	0.070	0.066
Iris	0.052	**0.043**	0.045	**0.043**	0.045	0.049	0.043	0.044	0.048	0.045	**0.043**	0.046
Liver	0.283	0.276	0.267	0.267	0.261	0.270	0.265	0.277	**0.253**	0.259	0.259	0.272
Lymph	0.177	0.168	0.168	0.165	0.153	0.149	**0.145**	0.151	0.161	0.149	0.168	0.162
Sonar	0.228	0.241	0.218	0.231	0.211	0.206	0.207	0.195	0.194	0.190	0.191	**0.181**
Vehicle	0.194	0.192	0.187	0.183	0.183	0.185	0.177	**0.176**	0.182	0.183	0.218	0.179
Vote	0.043	0.046	0.045	0.043	0.041	0.043	**0.040**	0.042	0.046	0.042	0.048	0.048
Vowel	0.008	0.013	**0.007**	0.011	0.009	0.009	0.012	0.013	0.011	0.012	0.015	0.030
Wbc	0.030	0.029	0.028	0.031	0.029	0.034	**0.028**	0.032	0.030	0.034	0.032	0.038
Wine	0.042	0.038	0.019	**0.015**	0.024	0.020	0.020	0.025	0.017	0.022	0.191	0.035
Average Error	0.148	0.156	0.139	0.148	0.135	0.146	**0.133**	0.143	**0.133**	0.141	0.153	0.141
Wins	9	6	9	6	9	6	10	5	8	7	7	8
Average Rank	7.87	7.93	5.53	6.40	4.80	7.07	**3.33**	6.00	4.87	5.87	8.47	8.40
p-values	0.9333		0.9669		0.8682		0.8357		0.9339		0.604	

3.2 Discussion of Results

We have presented the results of the double subagging ensemble from now on we shall denote this as DSB, with selection method in Table 2, then in Table 3 we have showed the results of the overall comparison of the best performing DSB

with other popular ensemble methods. For convenience we define the notations we used in the tables:

1. DSBXX= Double Subagging (embedded selection method) with SSR = XX
2. SBXX = Subundling with SSR = XX
3. Dbag = Original Version of Double Bagging
4. Bundle = Original Version of Bundling
5. LSVMXX = Double Subagging with LSVM as the additional classifier with SSR = XX
6. DSBADDCLAS = Double Subagging (embedded selection method) with additional classifier ADDCLAS

In Table 2 we have reported the pairwise wins of DSBXX vs SBXX with same SSR. From these values we see that in all the cases except for Dbag and Bundle, DSB has superiority (more wins than loses) over SB. The criteria for conducting the Nemenyi test is invalid for this table, so we could not conduct that. Based on the value of average errors and average ranks DSB40 is the best method in this table. From the p-values of Wilcoxon test we can say that the difference between the performance of DSB40 and SB40 is different where as the others are not so significant. The other important thing to notice in this table is that, the

Table 3. Comparison of error rates of Bagging, Adaboost, DSB40, LSVM40, SB50 and Rotation Forest in benchmark datasets

Datasets	Bagging	Adaboost	DSB40*	LSVM40	Sbundle50	Rotation Forest
Diabetes	0.2820	0.2929	**0.2331**	0.2460	0.2501	0.2531
German	0.2992	0.3300	**0.2254**	0.2310	0.2314	0.2847
Glass	0.2453	0.2456	0.2243	**0.2231**	0.2536	0.2439
Heart	0.3037	0.2336	0.1588	0.1570	**0.1543**	0.1754
Hearts	0.2874	0.2191	**0.1630**	0.1670	0.1746	0.2109
Ion	0.0832	0.0695	0.0587	0.0678	0.0700	**0.0559**
Iris	0.0747	0.0533	**0.0427**	0.0507	0.0503	0.0432
Liver	0.3177	0.3059	0.2649	0.2759	**0.2636**	0.2968
Lymph	0.1775	0.1602	**0.1446**	0.1459	0.1536	0.1557
Sonar	0.2289	0.1798	0.2067	0.2192	0.1954	**0.1726**
Vehicle	0.2525	0.2368	**0.1773**	0.2090	0.1880	0.2182
Vote	0.0515	0.0508	0.0405	**0.0402**	0.0473	0.0422
Vowel	0.0855	0.0517	**0.0119**	0.0473	0.0171	0.0511
Wbc	0.0299	0.0331	**0.0284**	0.0325	0.0387	0.0289
Wine	0.0315	0.0331	**0.0202**	0.0231	0.0275	0.0307
Average Error	0.1834	0.1664	**0.1334**	0.1424	0.1410	0.1509
Average Rank	5.47	4.93	**1.60**	2.60	3.20	3.20
CD(Critical Difference) = 1.58 , DF(difference in average ranks between best and worst method)=4.06						
Groups	Group 3	Group 3	Group 1	Group 1	Group 2	Group 2
p-values	0.0815	0.2133		0.7242	0.7716	0.4807
*= The best performing ensemble considering best average rank in accuracy and time to train						

DSBLSVM is selected most of the times in all the datasets, indicating that LSVM optimize the performance of double subagging than other additional classifiers.

For the second experiment we have selected DSB40 based on its performance, SB50 as it has the best performance among the subundling ensembles to compare with bagging, adaboost and rotation forest. As the DSBLSVM is selected in most of the times in the previous experiment, we have also included LSVM40 just to check its performance with other ensembles. From the average errors and average ranks we can see that DSB40 has far better performance than rotation forest, which is considered as one of the most accurate ensemble method now a days. LSVM40 is the second most accurate ensemble after DSB40, its performance is also better than rotation forest in most of the datasets. In this experiment we could conduct the Nemenyi test, we find out that there is no significant difference between DSB40 and LSVM40, where as rotation forest and SB50 also has no significant difference also the same for bagging and adaboost.

4 Conclusion and Future Research Direction

Embedding cross-validation inside double subagging to select the ensemble with optimum additional classifier greatly increases the performance of the respective ensemble. The benefit is mainly due to having more data for hillclimbing, the other reason for the success is having a larger OOBS to train the additional classifier model. From our experimental results it is clear that the performance of double bagging can be remarkably increased with the optimum selection of an additional classifier and a larger OOBS. We used four additional classifier models in the additional classifier pool of double bagging, and from selection point of view, the double subagging with LSVM is being selected most of the times, so it can also be concluded that double subagging with LSVM can be used also without the selection procedure. The performance of the double subagging with selection of optimum additional classifier is far better than all of the latest ensemble methods, e.g., rotation forest, adaboost, bagging, where as double subagging with LSVM also performing better in most of the cases than these ensemble methods. These results indicate that there are some areas where the performance of the double subagging ensemble can be increased further:

1. Though the performance of the double subagging ensemble differ slightly between SSR 0.3, 0.4 and 0.5, we can select the optimum SSR by the embedded cross-validation method.
2. We can run the ensemble selection method exhaustively, i.e., make a pool of additional models comprised of models with all the values of the parameters and then use this embedded cross-validation to select the optimum models from that additional model pool. To enhance the performance we can impose with replacement selection, so that better models are selected again and again, implying better performance of the ensemble.

3. We can select the additional classifier models (models only not the ensembles) based on their inbag error. We are running an experiment on this criterion at this moment. It can be extended to the selection of the optimum sample size of the inbag and OOBS.

Acknowledgments. This work has been partially supported by the Grant-in-Aid for Scientific Research (A) No.19200004 of the Ministry of Education, Science, Sports and Culture (MEXT) from 2007 to 2010.

References

1. Blake, C.L., Merz, C.J.: UCI Repository of Machine Learning Databases, http://www.ics.uci.edu/mlearn/MLRepository.html
2. Breiman, L.: Bagging predictors. Machine Learning 24(2), 123–140 (1996a)
3. Breiman, L.: Out-of-bag estimation. Statistics Department, University of Berkeley CA 94708, Technical Report (1996b)
4. Breiman, L.: Random Forests. Machine Learning 45(1), 5–32 (2001)
5. Caruana, R., Niculescu-Mizil, A., Crew, G., Ksikes, A.: Ensemble selection from libraries of models. In: Proceedings of the 21st Int'l Conf. on Machine Learning (2004)
6. Caruana, R., Niculescu-Mizil, A.: Getting the most out of ensemble selection. In: Proceedings of the Int'l Conf. on Data Mining, ICDM (2006)
7. Demšar, J.: Statistical comparisons of classifiers over multiple datasets. J. Mach. Learn. Research 7, 1–30 (2006)
8. Dietterich, T.G.: Machine-learning research: Four current directions. AI Magazine 18(4), 97–136 (1997)
9. Freund, Y., Schapire, R.: Experiments with a New boosting algorithm. In: Machine Learning: Proceedings to the Thirteenth International Conference, pp. 148–156. Morgan Kaufmann, San Francisco (1996)
10. Freund, Y., Schapire, R.: A decision-theoretic generalization of online learning and an application to boosting. J. Comput. System Sci. 55, 119–139 (1997)
11. Hastie, T., Tibshirani, R., Freidman, J.: The elements of statistical learning: data mining, inference and prediction. Springer, New York (2001)
12. Hothorn, T., Lausen, B.: Double-bagging: combining classifiers by bootstrap aggregation. Pattern Recognition 36(6), 1303–1309 (2003)
13. Hothorn, T., Lausen, B.: Bundling classifiers by bagging trees. Comput. Statist. Data Anal. 49, 1068–1078 (2005)
14. Kuncheva, L.I.: Combining Pattern Classifiers. Methods and Algorithms (2004)
15. Rodríguez, J., Kuncheva, L.: Rotation forest: A new classifier ensemble method. IEEE Trans. Patt. Analys. Mach. Intell. 28(10), 1619–1630 (2006)
16. Zaman, F., Hirose., H.: Double SVMbagging: A subsampling approach to SVM ensemble. To appear in Intelligent Automation and Computer Engineering. Springer, Heidelberg (2009)
17. Zaman, F., Hirose., H.: Effect of Subsampling Rate on Subbagging and Related Ensembles of Stable Classifiers. In: Chaudhury, S., et al. (eds.) PReMI 2009. LNCS, vol. 5909, pp. 44–49. Springer, Heidelberg (2009)
18. Zaman, F., Hirose., H.: A Comparative Study on the Performance of Several Ensemble Methods with Low Subsampling Ratio. In: Accepted in 2nd Asian Conference on Intelligent Information and Database Systems, ACIIDS 2010 (2010)

Personalization of Search Profile Using Ant Foraging Approach

Pattira Phinitkar and Peraphon Sophatsathit

Advanced Virtual and Intelligent Computing (AVIC) Research Center
Department of Mathematics, Faculty of Science
Chulalongkorn University, Bangkok 10330, Thailand
pattirap@gmail.com, peraphon.s@chula.ac.th

Abstract. This paper proposes a three-stage analysis of web navigation that yields search results being relevant to the user's interests and preferences. The approach is inspired by ant foraging behavior. The first stage focuses on a user's profile based on the web pages visited to be proportional with the amount of pheromone deposited by the ants. The level of pheromone denotes scores of user's interest. The second stage classifies the user's profile data. The final stage personalizes the search results based on the user's profile. Search results, which may span across a wide range of document archives and scatter over the Internet, will then be logically grouped by category for easy access and meaningful use. The experiments mainly consider the search results with reference to the user's profile in presenting the most relevant information to the user.

Keywords: search profile, search personalization, word similarity, Ant Colony Foraging.

1 Introduction

As the volume of information grows rapidly on the Internet, more investment on web search engines follows suit. Unfortunately, the number of search results usually turns out to be unsatisfactory. Often times, users must go through a long listing of documents to look for a few relevant ones. Determining the relevance of search results mostly relies on the user's own background and search context, e.g., the search result of "palm" yields more information on the Personal Digital Assistant (PDA) than a palm tree. Bearing such issues of user's interests and preferences (hereafter will be referred to as "user's profile") in mind, this paper provides a straightforward approach to build a user's profile based on interest scores which are derived from pheromone deposited by the ants. This profile reflects the user's behavior as pheromone being accumulated or evaporated. In the mean time, the content keywords of user's profile are classified in a reference concept hierarchy. A set of experiments was devised to carry out personalized search according to the proposed approach, yielding satisfactorily results.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 209–224, 2010.

The paper is organized as follows. Section 2 briefly recounts some related work. The proposed approach is procedurally elucidated in Section 3, along with the supporting experiments in Section 4. Some final thoughts and future challenges are given in Section 5.

2 Related Work

There have been numerous improvement challenges to personalize web mechanisms offered by search engines over the last few years. This is because people are naturally unwilling to spend extra efforts on specifying their intention. One approach to personalization is to have the users describe their own interests. Other approaches to automatic characterization use the user's profile derived from their interests and preferences. All pertinent information being extracted is then used to create a personal profile for setting designated queries on web page. Jaime, et al [1] explores rich models of user's interests built from both search-related and personal information about the user. We focus on personalization search results without having to be over expressive on user's interest.

One essential step in the improvement procedure is classification of personalized information. The classification process is to organize disordered information in a methodical arrangement. Emily, et al [2] proposes a method to classify queries by intent (CQI). Knowing the type of query intent greatly affects the returning relevant search results.

A prevalent shortcoming of search process is that many personal search approaches often return search results by focusing on the user's interests and preferences rather than on user's queries. The underlying principle utilizes personal profiles in the search context to re-rank the search results for furnishing more relevant outcomes to the users. The search process and ranking of relevant documents are achieved by contextual search based on the user's profile. Amiya, et al [3] presents a system architecture that would work as a subordinate to a normal search engine by taking its results, calculating the relevance of these results with respect to the user's profile, and displaying the results along with its relevance to the user. Ahu, et al [4] demonstrates that re-ranking the search results based on user's interest is effective in presenting the most relevant results to the user.

3 Proposed Approach

The focus of this work is to provide the most relevant search results to a user by personalization search according to his profile. Our approach will adopt ant colony foraging algorithm to perform both gathering the user's interests and updating the user's profile.

The proposed approach consists of three main steps, namely, building the user's profile, classifying the user's profile data, and personalization the search results by means of the user's profile as illustrated in Figure 1. The analysis will proceed in two systematic processes, namely, coarse-grained overview and fine-grained scrutiny.

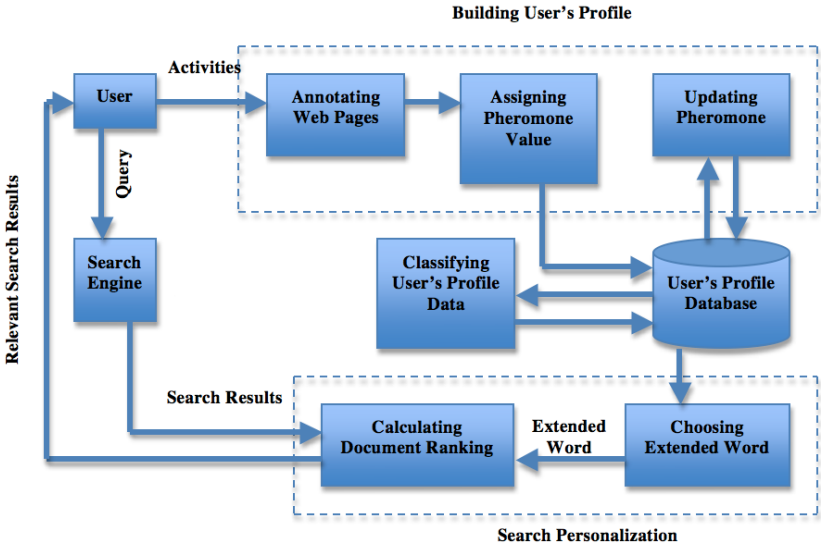


Fig. 1. Architecture of the proposed approach

3.1 Building User's Profile

A user's profile represents the user's interests and preferences in order to deduce user's intention for queries. In our approach, a user's profile consists of a set of categories, each of which encompasses a set of elements and its corresponding weight. Each category denotes the user's interest in that category. The weight or score of user's interest in an element represents the significance of that element with respect to the category.

The fundamental principle of user's profile creation is inspired by the nature of ant colony foraging behavior [5]. The ant leaves pheromone chemical as a communication means. Ants will typically choose to lay pheromone depending on the quality and quantity of food found at a source when foraging for food. Consequently, a strong pheromone path is created as soon as a profitably high value of food source is found. In general, the stronger value of pheromone it produces, the less pheromone evaporates. As food sources become depleted, it is to the advantage of the colony for the pheromone to evaporate over time. This eliminates the possibility of ants following a strong pheromone trail to a food source that has already been diminished. It follows then that, in a situation where there is a certain probability of food randomly appearing, the colony could find new food sources.

By the same token, the user's profile is changing periodically. Thus, to solve the problem by optimizing of the pheromone level of concentration, a pheromone update is required to keep the user's profile up to date at all time. Bearing this notion in mind, assuming that web page destinations portray the food sources, the system adds the interest scores to the user's profile as pheromone gets deposited when the user visits the destination web pages. As such, the amount of pheromone being deposited depends on the user's interest of the destination web page, particularly for the pages that are located deep under the home page links of interest.

The creation of user's profile serves as a coarse-grained process that exploits pheromone deposit technique to arrive at a user's interest summary and efficient search results.

3.1.1 Annotating Web Page

When a user visits the destination web page, information must be extracted to annotate web page contents. Using full text documents to annotate web page takes considerable amount of time. Hence, our approach extracts information from parts of HTML document. Since a web page is a semi-structured document, annotation of web page contents is determined by the structure of the web pages. To confine the size of search space, the proposed approach considers only three kinds of tags and attributes from HTML pages, namely, URL, tag<title>, and tag<meta name="description">. URL is selected because not only navigation path can be traced from the URL, but also web page contents are usually related to their source. The URL strings accurately describe what is contained in each folder by means of descriptive words to enhance intuitive meaning to the user as shown in Figure 2. The tag<title> and tag<meta name="description"> provide descriptions of the web pages. The tag<title> gives a brief definition of the web page, whereas the tag <meta name="description"> provides a concise explanation of the content of web page. The proposed approach looks for the most redundant words to apply annotation of the page. For example, if the most redundant word is football, one criterion on page annotation is to choose the web page annotated with football. Another criterion is to employ page type classification that is determined by the pheromone count. The procedure will be described in subsequent sections. At any rate, a systematic procedure for participating candidate word consideration that is produced by tags and attributes is the root word, disregarding all derivatives thereof.

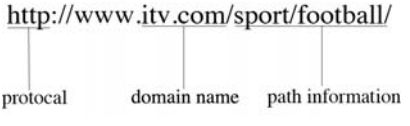


Fig. 2. A dichotomy of a URL

In this approach, URL, tag<title>, and tag<meta name="description"> are segmented into tokens. The procedure breaks non-alphanumeric characters, conjunction words, and stop words to create smaller tokens, and applies Porter stemming algorithm [6] to transform each token to a root word. An indicative statistics, that is, word density is computed from these tokens to gather web page annotation statistics.

Word density can be computed from the equation:

$$\text{density} = ((Nkr * Nwp) / Tkn) * 100 . \quad (1)$$

where Nkr denotes word frequency, Nwp is number of word occurrences in a phrase, and Tkn is the total number of words.

The sample web page annotation is shown in Table 1. Each URL, tag, and meta tag are segmented into tokens and assigned weight derived from the previous density statistics as shown in Table 2.

Table 1. Sample web page with URL, tag, and META tag

URL	Tag<title>	Tag<meta name="description">
http://news.bbc.co.uk/sport2/hi/football/default.stm	BBC SPORT | Football	The latest BBC Football news plus live scores, fixtures, results, tables, video, audio, blogs and analysis for all major UK and international leagues.

Table 2. Weight and density of individual token

Tokens	Weight	Density
news	1,1	10.526
sport	1,1	10.526
hi	1	5.263
football	1,1,1	15.789
:	:	:
league	1	2.263

3.1.2 Assigning Pheromone Value

The analogy of quality of the food source that affects the amount of pheromone deposit gives rise to the pheromone value of user's interest in the web page. Typically, most users prefer a direct link to the web page that they are interest in. However, if they cannot find sufficient information required to reach the designated web page, they will surf through the web pages to find the desired information. Consequently, counting the path along the URL measures the user's interest in the web page. The frequency of visiting the same type of web pages can also be used to evaluate user's concentration. These two factors constitute the pheromone value of the designated web page.

One essential ant foraging behavior occurs when ants found a good quality food source. They will congregate at the food source to acquire as much food as they can. Thus, heavy pheromone will be deposited along the path to food source. By this analogy, we also consider the selected web pages acquired from search results as an additional factor of pheromone value calculation.

In creating a new user's profile, the above information so obtained is inadequate to infer what the user real interests are. Fortunately, the selected web pages can make up "short-term" user's interests. By assigning higher weight to increase the amount of pheromone deposit, the level of information in the user's profile will quickly become steady for inference of user's interest.

As the user's interest diverts over a period of time, these short-term interest surges will gradually subside. The corresponding assigned weight will also decrease (or evaporate). This is called a "long-term" user's interest. Switching between short-term and long-term user's interest determined by the rate of pheromone evaporation, which will be further elaborated in next section. The rationale behind this observation is to

render a newly created user's profile reaching steady state as soon as possible in proportional to the selected web pages (or pheromone deposit). When the surge subsides so does pheromone deposit amount as they evaporate.

Table 3 shows sample frequencies of visiting web pages. Each node represents the web page annotated from the previous step. The amount of pheromone deposit denotes the frequency of visit, which includes the same type of web page. The most visited node is technology node as shown in the table, reflecting higher user's interest in technology topic than the rest of the topics under investigation.

Table 3. Pheromone deposition of visit

No.	Node	Amount of pheromone deposit
1	Technology	37
2	Football	29
3	System Analysis	20
4	Car	8
5	Camera	5
6	Game	3

3.1.3 Updating Pheromone

As user's interests and preferences always change over time, the value of pheromone must be updated, preferably in real-time, to keep the user's profile up-to-date. According to ant colony behavior, deposit and evaporation of pheromone must be proportionated. If the destination has abundant food source, many ants will go there and lay pheromone which results in strong pheromone deposit and lower evaporation rate along the path. On the other hand, for a low quantity of food source, the path will make a weak pheromone path having high evaporation rate because few ants will visit the area.

When the rate of pheromone evaporation for the node becomes 1, or the highest of the rate of pheromone evaporation, that node will be deleted from the user's profile. The fact is that the user has lost interest in that topic.

The formula for pheromone value update, or equivalently the user's interest score, can be determined as follows:

$$\tau_d = (1 - \rho)\ \tau_d\ . \tag{2}$$

where τ_d denotes the amount of pheromone on a given destination web page and ρ denotes the rate of pheromone evaporation. The equation of the rate of pheromone evaporation (ρ) is

$$\rho = 1 - (\tau_d / \Sigma\tau_d)\ . \tag{3}$$

In this paper, we adjust the pheromone differences to accommodate subsequent computations by the equation:

$$\tau_d = (1 - \rho)\ \tau_d^{\ \alpha}\ . \tag{4}$$

3.2 Classifying User's Profile Data

After annotating the web pages and collecting user's interest to be archived in the user's profile, some of this information may be similar by category, others may be different. Organizing this information for fine-grained scrutiny is a necessary requirement to keep track of the objects of similar properties, as well as their relationships if they exist. In other words, it is an issue of how this information should appropriately be classified. In so doing, performance of the personalization process will improve. The proposed approach employs WordNet [7] to establish a user's preference word-list, and Leacock-Chodorow measure [8] for semantic similarity in the classification process.

Leacock-Chodorow measure deals with semantic similarity by only considering the IS-A relation. To determine semantic similarity of two synsets, the shortest path between the two synsets in the taxonomy is determined and scaled by the depth of the taxonomy. The following formula computes semantic similarity:

$$\text{Sim}_{\text{LCH}}(a,b) = -\log(\text{length}(a,b) / (2 * D)) . \quad (5)$$

where length denotes the length of the shortest path between synset *a* and synset *b*, and D denotes the maximum depth of the taxonomy.

Leacock-Chodorow measure assumes a virtual top node dominating all nodes and will always return a value greater than zero, as long as the two synsets compared can be found in WordNet. Leacock-Chodorow measure gives a score of 3.583 for maximum similarity that is the similarity of a concept and itself.

Table 4. Similarity value of word-list from user's profile

	football	cruise	tour	tennis	travel	resort	sport	game	seafood
football	-	1.1239	1.2040	1.8971	1.3863	1.7430	*2.5903*	2.3026	1.1239
cruise	1.1239	-	1.9459	1.1239	*2.6391*	2.2336	1.7228	1.3863	0.8557
tour	1.2040	1.9459	-	1.2040	*2.6391*	1.5404	1.5404	1.6094	1.2910
tennis	1.8971	1.1239	1.2040	-	1.3863	1.7430	2.3026	2.3026	0.9808
travel	1.3863	*2.6391*	*2.6391*	1.3863	-	*2.6391*	1.9459	1.743	1.2040
resort	1.7430	2.2336	1.5404	1.7430	*2.6391*	-	2.0794	2.3026	1.3863
sport	*2.5903*	1.7228	1.5404	*2.3026*	1.9459	2.0794	-	*2.5903*	1.6094
game	2.3026	1.3863	1.6094	2.0794	1.7430	2.3026	*2.5903*	-	*2.3026*
seafood	1.1239	0.8557	1.2910	0.9808	1.2040	1.3863	1.6094	2.3026	-

The first step of classifying the user's profile is to compute similarity value from Equation (5) by setting up a word-list matrix created from the user's profile. A word-pair similarity value so computed indicates the closeness between the designated word-pair. The results are shown in Table 4.

The second step creates a bipartite graph designating the classification of word relations that build from the most similarity value of each designated word-pair. Each designated word-pair, which is selected to build a bipartite graph, is called word-list. The upper hierarchy represents category name which is derived from the nodes having common characteristics. The lower hierarchy of category name represents the corresponding elements.

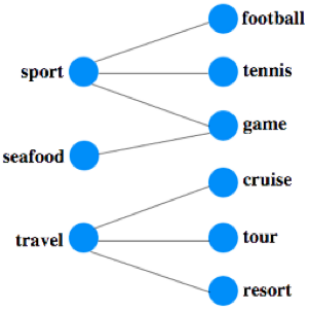


Fig. 3. An example of a bipartite graph with category name and its elements

Figure 3 depicts a sample bipartite graph of category name and its elements. To check whether an element belongs to the right category, the relationship between category name and its element must exist. If any element does not have a word-list relation, the element does not belong to its category and will be removed from the category and placed on unclassified category as shown in Table 5. For example, in Figure 3, sport– football, sport – tennis, sport – game, and game – seafood are element-category pairs. It appears that sport – game – seafood are related. However, sport – seafood does not contain in word-list relationship pair, thus seafood does not map to sport category.

Table 5. Category and its element

Category name	Element
sport	football, tennis, game
travel	cruise, tour, resort
-	seafood

To test the proposed approach classification capability, we compared our directory with Yahoo [9] and Google directories [10]. The results are close to both Yahoo directory and Google directory searches as shown in Table 6a and 6b, but are smaller and less complex than those of Yahoo and Google. Our directory contains all relevant category names and their elements that are easy to comprehend.

Table 6a. Sport category comparison of Yahoo, Google, and our directory

Sport directory		
Yahoo directory	Google directory	Our directory
recreation> sport>football	sport> football	sport> football
recreation> sport>tennis	sport> tennis	sport> tennis
recreation> game	game	sport> game

Table 6b. Travel category comparison of Yahoo, Google, and our directory

Travel directory		
Yahoo directory	Google directory	Our directory
recreation> travel>cruise	recreation> travel>specialty travel>cruise	travel> cruise
recreation> travel>tour	recreation> travel>tour	travel> tour
recreation> travel>resort	recreation> travel>loading> resort	travel> resort

3.3 Search Personalization

A typical search query often ends up with plentiful results that contain few relevant ones. To reduce unwanted search results, the above user's profile classification can be exploited to establish a search personalization mechanism. Search personalization is based on user's interest subjects (described by single word) having the highest amount of pheromone deposit. By reordering the pheromone deposit, all subjects (words) can be arranged according to their relevance to suit the user's personal preference.

The proposed approach supports word query between nouns, verbs, adjectives, and adverbs. Word query can be a word or collocation of words in the form of a sequence of words that go concurrently for a specific meaning such as "system analysis and design". However, the proposed approach does not support sentence query. One may contend that the more query words used, the clearer the (meaning of) query. Nevertheless, most users do not like to enter too many words just to look for a piece of information, typically about 3 words [13]. As such, adding one or two "key" words to form an extended word (to be described subsequently) entails a keyword search approach that yields high performance and useful results. This is because the extended word will help narrow down search theme which enables the search engine to recognize the user's interests and preferences.

Search personalization is then carried out in two steps. The first step is to choose an extended word based on the user's profile to make a new query which is more relevant to the user. The second step is to rank the search results obtained from the first step. The results are sorted in descending order. The procedural details are described below.

3.3.1 Choosing Extended Word for Making a New Query Keyword

To analyze if a word in the user's profile can be used as an extended word, all words are first classified and formed a bipartite graph. Each node of the bipartite graph is assigned a weight which is the pheromone deposit of user's interest. All words in the bipartite graph hierarchy form an extended word list to match the input query search results, irrespective of individual word position. This is the first step of the search personalization process. Figure 4 illustrates a user's profile classification from the bipartite graph and the corresponding pheromone value. There are three matching scenarios to consider:

1. Matching category name with the query. The query matches a category name having the highest pheromone deposit. The element becomes the extended word.
2. Matching element with the query. The query matches an element that belongs to one or more categories. If the element belongs to one category, the element will match with its own category. Otherwise, the element will match with the category that has the highest pheromone deposit.
3. No matching word between the query and user's profile word-list. This scenario will choose a word having the highest pheromone deposit in the user's profile to be an extended word.

The above matching scenarios are exemplified by the following examples.

Scenario	Query word	Extended word
1	sport	sport, football
2	palm	palm, technology
3	news	news, technology

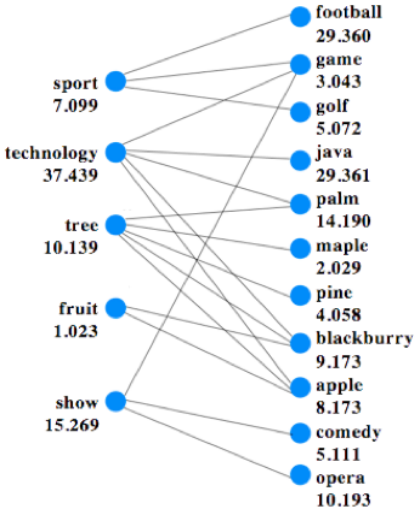


Fig. 4. A bipartite graph of category name and its elements with pheromone value

3.3.2 Calculating Document Ranking

The new extended query will yield search results that provide more relevant information to the users. Relevancy is obtained from re-ranking all words in the pertinent document, whereby the most likely related document will be retrieved.

To calculate ranking of each document, the cosine similarity between the extended query and the user's profile is computed. The cosine of two vectors is a measure of how similar two vectors will be on the (0,1) scale, where 1 means completely related (or similar) and 0 means completely unrelated (or dissimilar). The cosine similarity of two vectors *a1* and *a2* is defined as follows:

$$\mathrm{Sim}_{\cos}(a1, a2) = \cos(a1, a2) . \tag{6}$$

$$\cos(a1, a2) = \mathrm{dot}(a1, a2) / \|a1\| \|a2\| . \tag{7}$$

where *a1* denotes the extended query, *a2* denotes the term frequency of document, and dot(a1, a2) denotes the dot product of *a1* and *a2*. Term frequency, which measures how often an extended query is found in a document, is defined as follows:

$$\mathrm{tf}_{i,j} = \frac{n_{i,j}}{\sum_k n_{k,j}} . \tag{8}$$

where $n_{i,j}$ denotes the number of occurrences of the considered term (t_i) in document d_j and $\Sigma_k n_{k,j}$ denotes total occurrences of all terms in document d_j.

Table 7 depicts a new ranking of search results from the extended query "technology news" ordered by the most similarity to the least similarity.

Table 7. Using cosine similarity for re-ranking search results

Rank	Pervious rank	URL	Cosine similarity
1	2	http://edition.cnn.com/TECH/	0.99228
1	9	http://www.techweb.com/home	0.99228
2	7	http://news.zdnet.com/	0.99160
3	5	http://www.nytimes.com/pages/technology/index.html	0.85749
3	10	http://www.t3.com/	0.85749
4	6	http://www.businessweek.com/technology/	0.83957
5	8	http://www.physorg.com/technology-news/	0.80717
6	1	http://news.cnet.com/	0.79262
7	3	http://www.technewsworld.com/	0.70711
7	4	http://news.yahoo.com/technology	0.70711

4 Experiments

The experiments were carried out in different stages, namely, experimental setup, annotating web page, assigning, updating pheromone value, and re-ranking. The outcomes were measured by their precision and tested against Yahoo [11] and Yahoo Motif [12].

4.1 Experimental Setup

Four sets of extensive experiments were conducted based on the proposed procedures described. The first set, involving a basic word "Technology" will be elucidated in the sections that follow. The remaining three sets, i.e., Zoology, Botany, and Finance were carried out in the same manner.

4.2 Annotating Web Page

Since evaluation of the proposed approach is based primarily on the frequency of user's web access, we annotated the web pages which the users visited and found that 81% of the annotated results was similar to the page title. Figure 5 shows the density of each token from sample web pages. From Figure 5, football is the selected annotated web page because it has the highest density.

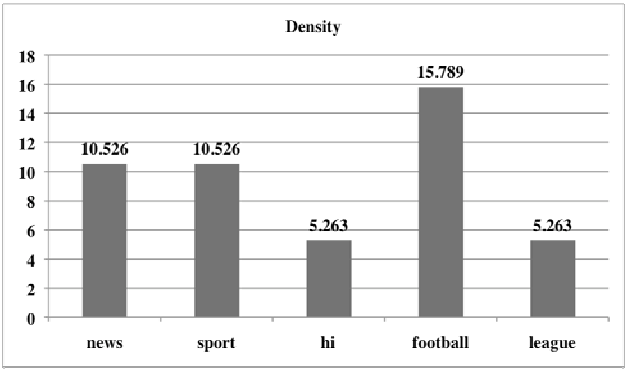


Fig. 5. Comparison of token density

4.3 Assigning and Updating Pheromone Value

The user's interests and preferences were determined from the amount of pheromone deposit, while the user's profile was kept up-to-date by the rate of pheromone evaporation. Thus, the updated pheromone value of each node in the bipartite graph would reflect the current degree of user's interest.

Table 8 summarizes the amount of pheromone deposit, rate of pheromone evaporation, and pheromone of each node. The higher the amount of pheromone deposit, the higher the degree of user's interest. The rate of pheromone evaporation is used to update the user's profile. Lower pheromone rate of evaporation reflects the intense of current user's interest, whilst higher pheromone rate of evaporation signifies the topics of interest currently being faded away. The pheromone represents the actual degree of user's interest.

Table 8. Pheromone deposit, rate of pheromone evaporation, and pheromone of each node

No.	Node	Amount of pheromone deposit	Rate of pheromone evaporation	Pheromone
1	Technology	37	0.561	37.439
2	Football	29	0.639	29.361
3	System Analysis	20	0.738	20.262
4	Car	8	0.887	8.113
5	Camera	5	0.928	5.072
6	Game	3	0.957	3.043

4.4 Re-ranking

Re-ranking process makes use of extended word notation based on user's interest and input query word. Using as few input keywords as possible, the user's profile is searched to retrieve the word having highest interest score to be combined with the input query word, or extended word in our context. Experiments were tested to compare simple query words with extended query words, and to compare Yahoo Motif with extended query words. For instance, the input query word "palm", along

with the highest interest scored word "technology", form an extended word "palm technology" for use in the search query. As a consequence, the search results yield different documents to be retrieved from a new list of URLs. This process is called re-ranking.

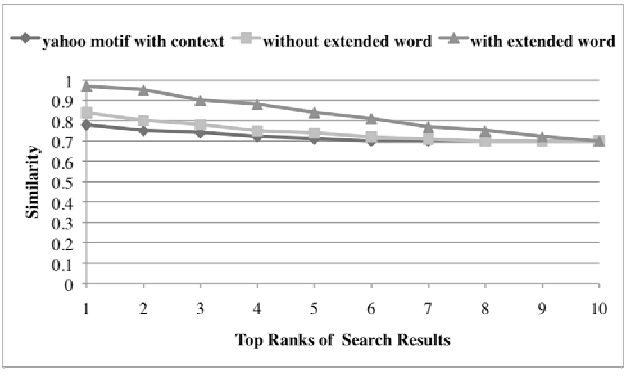


Fig. 6. Input (simple) query: palm, Yahoo motif query: palm, extended query: palm technology

Figure 6 shows the result comparison between query with simple query words, yahoo motif, and extended query words. The results of the three queries show that the last query yields more relevant documents to the user than the other two queries. A closer look at the cosine similarity value of the results reveals that the new ranking from extended word is closer to 1 than the ranking without extended word and Yahoo motif with context.

4.5 Experimental Results

Effectiveness of the proposed approach relates directly to the relevancy of retrieved results. The effectiveness of personalized search is measured by precision of the ability to retrieve top-ranked results that are mostly relevant to the user's interest. The precision is defined as follows:

$$\text{precision} = \frac{\text{number of relevant documents retrieved}}{\text{total number of documents retrieved}}. \quad (9)$$

For personalized search evaluation, we used four different user's profiles in each set of experiment. Some entries could appear in more than one profile as search went on. For example, "python" could fit either technology profile or zoology profile, "palm" could be in technology profile or botany profile, or "portfolio" could be in technology profile or finance profile. Table 9 compares the top-10 ranked of relevant search results based on user's profile. Table 10 shows the precision of the overall search results at different time. Those that are not relevant to the user's interest exhibit low precision values. However, as activities increase, search results improve since sufficient information is accumulated. This fact is depicted in Figure 7.

Table 9. Comparison of top-10 ranked relevant search results between Yahoo, Yahoo Motif, and our approach

Input query	Profile	Extended query	Amount of relevant results in top-10 ranked		
			Yahoo	Yahoo Motif	Our approach
palm	technology	palm technology	9	2	9
python	zoology	python snake	0	9	10
palm	botany	palm tree	0	2	8
portfolio	finance	portfolio finance	6	10	9

Table 10. The precision of user's profiles at different time

	Precision			
Time	Technology	Zoology	Botany	Finance
T1	0.5	0.0	0.0	0.6
T2	0.6	0.2	0.0	0.6
T3	0.7	0.3	0.1	0.6
T4	0.8	0.4	0.2	0.7
T5	0.8	0.5	0.3	0.7
T6	0.8	0.7	0.4	0.8
T7	0.9	0.8	0.6	0.8
T8	0.9	0.9	0.7	0.8
T9	0.9	1.0	0.8	0.9
T10	0.9	1.0	0.8	0.9

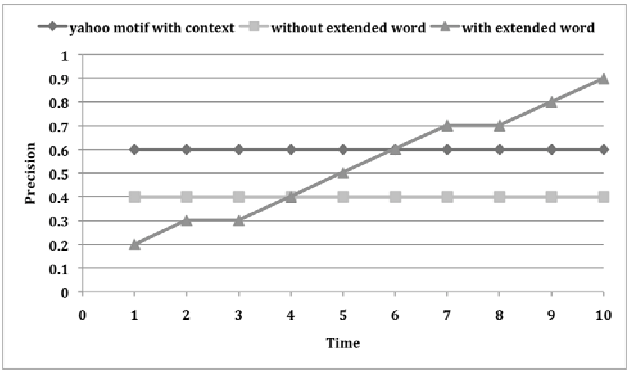


Fig. 7. Precision of personalized searches with extended word, general search without extended word and Yahoo Motif with context data

5 Conclusion and Future Work

We have presented the feasibility of personalized web search by means of an extended query that is automatically constructed from the most up-to-date user's

profile in accordance with the short-term and long-term interests. The short-term interest is induced by new events and vanishes quickly. On the contrary, the long-term interest generally reflects real user's interests. One way to realize this scheme is to set the short-term interest as the default search personalization and arrange the long-term interest as the secondary search. At a predetermined threshold period, short-term values are promoted to the long-term list. Older values in long-term list will eventually be discarded. Hence, search personalization will satisfy the user intent without having to resort to long strings of query.

The underlying principle was inspired by ant foraging behavior. When building a user's profile by extracting only the visited web pages and assigning a pheromone value as interest score, we found that the profiles converged to a stable set after approximately 350 visited web pages. On the other hand, if we incorporate the visited web pages and the selected web pages from the search results, the user profiles would converge to a stable set after approximately 100 visited web pages.

Our approach was tested on Yahoo and Yahoo Motif. The results yielded higher similarity score and precision score than those of Yahoo and Yahoo Motif, in particular, when comparisons were confined to the most relevant top-10 ranked results. However, a notable limitation of our approach is the performance which fell slightly as the profile contained less information, thereby the short-term compensation still fell short of what was anticipated.

There are no suitable personalization algorithms that fit all search queries. Different algorithms have different strengths and weaknesses. We will investigate in depth on extended words that exploit personalization algorithms to enhance the search results, whereby higher precision can be attained. Moreover, as the user gains more search experience, i.e., knowing how to select proper "search words", the precision score will increase. But this will take time to accumulate enough information before the steady state is reached. We envision that additional measures could be employed to shorten the profile accumulation cycle, namely, specificity, sensitivity, and accuracy, to see if the amount of information is sufficient for profile update, thereby user's experience will improve search profile personalization considerably.

References

1. Teevan, J., Dumais, T.S., Horvitz, E.: Personalizing search via automated analysis of interests and activities. In: Proceedings of the 28th annual international ACM SIGIR conference on research and development in information retrieval (SIGIR 2005), Salvador, Brazil, pp. 449–456 (2005)
2. Pitler, E., Church, K.: Using word-sense disambiguation methods to classify web queries by intent. In: Proceedings of the 2009 conference on empirical methods in natural language processing, Singapore, pp. 1428–1436 (2009)
3. Tripathy, K.A., Olivera, R.: UProRevs – user profile relevant results. In: Proceedings of the IEEE joint 10th international conference on information technology (ICIT 2007), pp. 271–276 (2007)
4. Sieg, A., Mobasher, B., Burke, R.: Web search personalization with ontological user profiles. In: Proceedings of the 16th ACM conference on information and knowledge management (CIKM 2007), Lisboa, Portugal, pp. 525–534 (2007)

5. Dorigo, M., Maniezzo, V., Colorni, A.: The ant system: optimization by a colony of cooperating agents. IEEE transactions on system, man, and cybernetics- part B 26(1), 29–41 (1996)
6. Porter, M.F.: An algorithm for suffix stripping. Program 14(3), 130–137 (1980)
7. WordNet, http://wordnet.princeton.edu/ (October 20, 2009)
8. Leacock, C., Chodorow, M.: Combining local context and WordNet similarity for word sense identification, ch. 11, pp. 265–283. MIT Press, Cambridge (1998)
9. Yahoo Directory, http://dir.yahoo.com/ (October 20, 2009)
10. Google Directory, http://directory.google.com/ (October 20, 2009)
11. Yahoo, http://www.yahoo.com/ (October 20, 2009)
12. Yahoo Motif, http://sandbox.yahoo.com/Motif/ (October 20, 2009)
13. Jansen, B.J., Spink, A., Bateman, J., Saracevic, T.: Real life information retrieval: a study of user queries on the web. ACM SIGIR Forum 32, 5–17 (1998)

A Novel Convinced Diffie-Hellman Computation Scheme and Its Cryptographic Application

Yuh-Min Tseng and Tsu-Yang Wu

Department of Mathematics, National Changhua University of Education,
Jin-De Campus, Chang-Hua 500, Taiwan
ymtseng@cc.ncue.edu.tw, d94211001@mail.ncue.edu.tw

Abstract. The Diffie-Hellman (DH) problem is an important security assumption in modern cryptography. In this paper, a new type of cryptographic technique called a convinced Diffie-Hellman (DH) computation scheme is proposed. In the convinced DH computation scheme, an issuer can convince a verifier that the computation of the Diffie-Hellman problem is correct under without revealing any exponential parts of two Diffie-Hellman public values. Firstly, the formal framework and security requirements for this new cryptographic scheme are defined. Then a concrete scheme is proposed. In the random oracle model and under the difficulty of computing discrete logarithm, we demonstrate that the proposed scheme meets the defined security requirements. Finally, we present an important application of the convinced DH computation scheme. Most group key agreement protocols provide only the functionality of detecting the existence of malicious participants, but don't identify who malicious participants are. The novel convinced DH computation scheme can be embedded in many multi-round group key agreement protocols to identify malicious participants and provide fault tolerance.

Keywords: Diffie-Hellman problem, convinced computation, malicious participant, group key agreement, cryptography.

1 Introduction

A key establishment protocol allows participants to establish a common key for encrypting their communications over insecure open networks. A two-party key exchange (or agreement) protocol is used to establish a common key for two parties, in which two parties contribute some information to derive the shared session key. In 1976, Diffie and Hellman [1] proposed the first two-party key agreement protocol. Up to now, the Diffie-Hellman (DH) problem is an important security assumption in modern cryptography. Its difficulty is closely related to solve the discrete logarithm problem over a cyclic group [2]. In the past, many variations of the DH problem were proposed such as square computational Diffie-Hellman (CDH) problem [3,4], inverse CDH proplem [5], and divisible CDH problem [6]. The relations between the DH problem and its variations, we can refer to [6] for a full description.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 225–235, 2010.

With the rapid growth of the Internet applications, the design of group key agreement (GKA) protocols has received increasing attention. A group key agreement protocol involves all participants cooperatively establishing a common key. In the past, many GKA protocols have been proposed and the security of most GKA protocols is based on the related assumptions of the Diffie-Hellman problem. These Diffie-Hellman-based protocols are classified into two kinds: non-authenticated [7,8,9,10,11,12,13] and authenticated [14,15,16,17,18]. In 2003, Katz and Yung [17] proposed a compiler that can transform any group key-exchange protocol into an authenticated protocol. Recently, insider attacks (or called malicious participant attacks) were well-defined in [19,20]. They presented the formal security definition of an authenticated GKA protocol in the existence of malicious participants. Adopting the complier in [19] into an authenticated GKA protocol, it can employ the explicit group key confirmation property to check the existence of malicious participants. However, these protocols cannot identify who malicious participant are, even if both authentication and key confirmation are involved in these protocols.

However, consider a situation in which there is an emergency, and some secure conferences must be held prior to a special time, such as military applications, rescue missions and emergency negotiations. In this case, the destruction of the conference could cause serious damage to many. If malicious participants try to disrupt the group key establishment, other honest participants will not be able to correctly agree on a common key. The common key will not be constructed and the secure conference will not be held, when honest participants cannot identify the malicious participant.

In [21], we have proposed a secure group key agreement protocol resistant to malicious participants. If there are any malicious participants who try to disrupt the group key establishment, they will be determined and deleted from the group. Other honest participants can re-run the GKA protocol to ensure the group key establishment and thus the proposed protocol provides fault tolerance. According to our previous result [21], we obtain a fact that group key agreement protocols based on the Diffie-Hellman problem [1] generally require multiple rounds to establish a common key, and each participant must compute the value of the Diffie-Hellman problem according to the received values in the previous round. If there exists a security scheme that allows a participant can convince other participants that he has correctly computed the Diffie-Hellman value without revealing any exponential parts, then identifying malicious participants will be reached.

In this paper, we generalize this approach of identifying malicious participants to propose a new type of cryptographic technique called a convinced Diffie-Hellman (DH) computation scheme. The proposed scheme can be embedded in other kinds of Diffie-Hellman-based group key agreement protocols to provide the functionality of identifying malicious participants. In the convinced DH computation scheme, an issuer can convince verifiers that he has correctly computed the Diffie-Hellman value without revealing any exponential parts. Since the convinced Diffie-Hellman computation scheme is a new security

mechanism, we firstly define the formal framework and security requirements. Then, a concrete scheme is proposed. In the random oracle model [22,23] and under the difficulty of computing discrete logarithm [2], we demonstrate that our convinced DH computation scheme meets the defined security requirements. Finally, one concrete deployment of the convinced DH computation scheme is given. We embed the convinced DH computation scheme in a GKA protocol to provide identifying malicious participants.

The remainder of this paper is organized as follows. In Section 2, we present the related security assumptions and notations. The framework and the security model of the convinced Diffie-Hellman computation scheme are given in Section 3. In Section 4, we present a concrete convinced DH computation scheme. In Section 5, we demonstrate security and performance analysis. One concrete deployment of the convinced DH computation scheme is presented in Section 6. Finally, conclusions are made.

2 Preliminaries

In this section, we present the related security assumptions and notations. The following notations are used throughout this paper:

- q: a large prime.
- p: a large prime such that $p = 2q + 1$.
- G_q: a subgroup of quadratic residues in Z_q^*, that is $G_q = \{i^2 | i \in Z_p^*\}$.
- g: a generator for the subgroup G_q.
- $H()$: a one-way hash function from Z_q to Z_q.

Here, we describe three number-theoretic problems in the group G_q with the prime order q. The security of the proposed scheme described in this paper relies on the following assumptions:

– *Decision Diffie-Hellman (DDH) assumption.* Given $y_a = g^{x_a} \bmod p$ and $y_b = g^{x_b} \bmod p$, where x_a and x_b are randomly chosen from Z_q^*, the following two tuples of random variables $(y_a, y_b, g^{x_a x_b} \bmod p)$ and (y_a, y_b, R), where R is a random value in G_q, are computationally indistinguishable.
– *Computational Diffie-Hellman(CDH) assumption.* Given $g^{x_a} \bmod p$ and $g^{x_b} \bmod p$, no probabilistic algorithm with non-negligible advantage within polynomial time can compute $g^{x_a x_b} \bmod p$.
– *Discrete Logarithm (DL) assumption.* Given $g^x \bmod p$, no probabilistic algorithm with non-negligible advantage within polynomial time can find the integer $x \in Z_q^*$.

3 Framework and Security Model

In this section, we define the formal framework and the security requirements of a novel convinced DH computation scheme.

3.1 Formal Framework

In the convinced DH computation scheme, there are two entities involved in this scheme: the issuer and the verifier. Informally, we first present an example of the convinced DH computation scheme. Given two Diffie-Hellman public values $y_a = g^{x_a} \bmod p$ and $y_b = g^{x_b} \bmod p$, where x_a and x_b are randomly chosen from Z_q^*, any user without knowing x_a or x_b will not distinguish $(y_a, y_b, Y = g^{x_a x_b} \bmod p)$ from (y_a, y_b, R), where R is a random value in G_q. This is a well-known DDH assumption. Assume that the issuer knows the secret x_a and the verifier knows neither x_a nor x_b. In the convinced DH computation scheme, the issuer releases a tuple σ including a value Y that allows the verifier to confirm $Y = g^{x_a x_b} \bmod p$. That is, the verifier without knowing x_a and x_b can be convinced that the issuer has computed the correct $Y = g^{x_a x_b} \bmod p$.

In the following, we present the formal definition of the convinced DH computation scheme. The convinced DH computation scheme can be viewed as a specific signature scheme with an addition property. As the same with classical signature schemes [24,25,26,27], the convinced DH computation scheme is made of the following three algorithms:

- *The key generation algorithm.* Given a security parameter l, the key generation algorithm produces the public parameters $Param = \{p, q, g, G_q, H()\}$ and a pair $(x \in Z_q^*, y = g^x \bmod p)$ of matching secret and public keys.
- *The issuing algorithm.* Given a message $m = g^z \in G_q$ for some $z \in Z_q^*$, $Param$ and a pair (x, y), the issuing algorithm produces a tuple σ including a special value $Y = g^{xz} \bmod p$.
- *The verifying algorithm.* Given a tuple $(m = g^z, y = g^x, \sigma)$ and $Param$, the verifying algorithm checks whether σ is valid on g^z with respect to the public key $y = g^x$. Meanwhile, the verifying algorithm can ensure $Y = g^{xz} \bmod p$. If both validations hold, the verifying algorithm outputs "True". Otherwise, it outputs "False". The verifying algorithm is not probabilistic.

3.2 Security Model

In the following, we present the security model of the convinced DH computation scheme. The security model consists of two security requirements: existential unforgeability and convinced computation property. We say that a convinced DH computation scheme is secure, if it satisfies two security requirements as defined below.

Definition 1. A convinced DH computation scheme offers **existential unforgeability** against adaptive chosen-message attacks if no probabilistic polynomial-time adversary A has a non-negligible advantage in the following game (EUF-CDHC-ACMA game) played between a challenger C and the adversary A.

- *Initialization.* The challenger C takes a security parameter l and runs the *key generation algorithm* of the convinced DH computation scheme to produce the public parameters $Param$ and a pair $(x \in Z_q^*, y = g^x \bmod p)$. Then C gives $Param$ and y to A.

- *Attack.* The adversary A may make a number of different types of queries in an adaptive manner as follows:
  - Hash query. Upon receiving the request query, C computes the value of the hash function for the requested input and sends the hash value to A.
  - Issuing query. The adversary A chooses an integer $m = g^z \in G_q$ and sends it to the challenger C. C produces σ and sends it to A.
- *Forgery.* The adversary A outputs (m^*, y, σ^*), where m^* and σ^* did not appear in previous issuing queries. If the response of the verifying algorithm on (m^*, σ^*) is "True", the adversary A wins the game. The advantage of the adversary A is defined as the probability that A wins.

In the convinced DH computation scheme, the issuing algorithm, given a message $m = g^z \in G_q$ and a secret key x, can produce a valid tuple σ including a specific value Y. If the verifying algorithm outputs "True", it can ensure that Y is equal to $g^{xz} \bmod p$. In other words, given a public value $m \in G_q$, an adversary with knowing the secret key x is unable to produce two valid tuples (m, y, σ_1) and (m, y, σ_2) including two different Y values, respectively. Therefore, the role of the adversary is simulated by the issuer with the secret key x in the convinced DH computation scheme. The **convinced computation** property is formally defined as follow.

Definition 2. A convinced DH computation scheme is said to have the **convinced computation** property if no probabilistic polynomial-time adversary A with knowing the secret key x has a non-negligible advantage in the following game (CDHC-CCP game) played between a challenger C and the adversary A.

- *Initialization.* The challenger C takes a security parameter l and runs the *key generation algorithm* to produce the public parameters $Param$ and a pair $(x \in Z_q^*, y = g^x \bmod p)$. Then C gives $Param$ and (x, y) to A.
- *Challenge.* The challenger C chooses a random value $z \in Z_q^*$ and computes $m = g^z \bmod p$, and then sends m to the adversary A.
- *Response.* Upon receiving m, the adversary A with knowing the secret key x produces a tuple σ including a special value Y. Then, A sends σ to C. The challenger C runs the verifying algorithm on (m, y, σ) and computes $y^z \bmod p$. If the output of the verifying algorithm is "True" and $Y \neq y^z \bmod p$, the adversary A wins the game. The advantage of the adversary A is defined as the probability that A wins the CDHC-CCP game.

4 A Convinced DH Computation Scheme

Here, we present a concrete convinced DH computation scheme. There are two entities in the proposed scheme: the issuer and the verifier. The issuer performs the issuing algorithm and the verifier runs the verifying algorithm. Without loss of generality, let $m = g^z \bmod p$ for some $z \in Z_q^*$ be the message. The detailed description of the proposed scheme is presented as follows:

[The Key Generation Algorithm]. The system has the following public parameters p, q, g, and $H()$ as defined in Section 2. Any issuer U_a with identity ID_a has a pair ($x_a \in Z_q^*, y_a = g^{x_a} \bmod p$) of matching secret and public keys. The issuer keeps x_a in secret and publishes the corresponding public key y_a.

[The Issuing Algorithm]. Given $m = g^z \in G_q$, the issuer with a pair (x_a, y_a) randomly selects an integer $r \in Z_q^*$ and computes the following values: $Y = (m)^{x_a} \bmod p$, $\alpha = g^r \bmod p$, $\beta = (m)^r \bmod p$, $h = H(y_a, m, Y, \alpha, \beta)$, and $\delta = r + hx_a \bmod q$. Then, the issuer sends $(m, y_a, \sigma = (Y, \alpha, \beta, \delta))$ to the verifier.

[The Verifying Algorithm]. Upon receiving (m, y_a, σ), the verifier checks whether both $g^\delta = \alpha y_a^h \bmod p$ and $(m)^\delta = \beta Y^h \bmod p$ hold or not, where $h = H(y_a, m, Y, \alpha, \beta)$. If two checks hold, the verifier can ensure that Y is equal to $g^{x_a z} \bmod p$.

5 Analysis

5.1 Security Analysis

As defined in Subsection 3.2, the convinced DH computation scheme is secure if it satisfies both existential unforgeability and convinced computation.

[Existential Unforgeability]. The random oracle model [22,23] is usually adopted to demonstrate the security of key establishment protocols or signature schemes by assuming that a hash function is actually a random function. If the same query is asked twice, identical answers should be obtained. In [26,27], Pointcheval and Stern used a forking lemma in the random oracle model to prove the security of signature schemes. This lemma adopts the "oracle replay attack" using a polynomial replay of the attack with the same random tape and a different oracle. Two signatures of a specific form are obtained to create a way to solve the underlying hard problem. In the random oracle model, by adopting forking lemma, we prove that the proposed scheme offers existential unforgeability under the assumption of the difficulty of computing discrete logarithm.

Theorem 1. *In the random oracle model, assume that adversary A with a non-negligible advantage can forge a valid tuple T for adaptive chosen-message attacks to the proposed convinced DH computation scheme. Then, there exists an algorithm C with a non-negligible advantage that can solve the computing discrete logarithm problem.*

Proof. Without loss of generality, assume that the algorithm C receives a random instance ($p, q, g, y_a = g^{x_a} \bmod p$) and he/she must compute the integer x_a. C acts as a challenger in the EUF-CDHC-ACMA game. The challenger C needs to maintain two lists L_1 and L_2 that are initially empty and are used to keep track of answers to $H()$ and issuing queries, respectively.

At the beginning of the game, the challenger C gives the public parameters and y_a to the adversary A. The challenger C is responsible to answer the different queries of the adversary A as follows:

- $H()$ query. Upon receiving the hash query request $H(\tau)$ from the adversary A, the challenger C searches a pair (τ, R_h) in the list L_1. If such a pair is found, C returns R_h. Otherwise, he returns a random value $R_h \in_R \{0,1\}^w$, where w is the output length of the hash function $H()$. Meanwhile, C adds (τ, R_h) into the list L_1.
- Issuing query. The adversary A chooses a $m = g^z \bmod p \in G_q$ and sends it to the challenger C. The challenger C produces a tuple $T = (m, y_a, \sigma = (Y, \alpha, \beta, \delta))$. C first randomly generates two value r_k and x_k from Z_q^*. Then C computes $(Y, \alpha, \beta, \delta)$ as follows: $Y = (m)^{x_k} \bmod p$, $\alpha = g^{r_k} \bmod p$ $\beta = (m)^{r_k} \bmod p$, and $\delta = r_k + hx_k \bmod q$, , where h is the simulated value of $H()$ query as the mentioned above. Finally C returns $T = (m, y_a, \sigma = (Y, \alpha, \beta, \delta))$ to the adversary A as the answer.

Following the Forking Lemma in [26,27], assume that A without knowing x_a can generate the correct $(m, y_a, \sigma = (Y, \alpha, \beta, \delta))$ with a non-negligible probability ϵ. Under the random oracle model, for any specific (m, y_a), A can generate two valid tuples $T = (m, y_a, \sigma = (Y, \alpha, \beta, \delta))$ and $T' = (m, y_a, \sigma' = (Y, \alpha, \beta, \delta'))$ with a non-negligible probability at least $\epsilon/2$ such that four equations $g^\delta = \alpha y_a^h \bmod p$, $(m)^\delta = \beta Y^h \bmod p$, $g^\delta = \alpha y_a^{h'} \bmod p$, and $(m)^{\delta'} = \beta Y^{h'} \bmod p$, where h and h' are two hash values of $H(y_a, m, Y, \alpha, \beta)$. Hence, A can obtain $\log_g(y_a) = \frac{\delta - \delta'}{h - h'}$. That is, the adversary A can compute the secret value x_a from y_a. Thus, the challenger C can run A as a subroutine to obtain x_a from the random instance $(p, q, g, y_a = g^{x_a} \bmod p \in G_q)$, which is a contradiction for the assumption of the difficulty of computing discrete logarithm. □

[Convinced Computation]. For the convinced computation property, given a message $m = g^z \bmod p \in G_q$ and a secret key x_a, an issuer can produce a valid tuple σ including a specific value Y. Any verifier can ensure that Y is equal to $g^{x_a z} \bmod p$. That is, if no adversary with the secret key x_a can produce a valid tuple σ with a value $Y \neq g^{x_a z} \bmod p$, then the proposed scheme provides convinced computation property.

Theorem 2. *In the random oracle model and under the difficulty of computing discrete logarithm, no adversary A with the secret key x_a can produce a valid tuple σ with a specific value $Y \neq g^{x_a z} \bmod p$ on the input $m = g^z \bmod p$.*

Proof. Without loss of generality, let the input be $m = g^z \bmod p$ for some integer $z \in Z_q^*$. By contradiction proof, we assume that the adversary A with the secret key x_a can take a random value r to perform the issuing algorithm in the proposed scheme to produce a valid tuple $T = (m, y_a, \sigma = (Y, \alpha, \beta, \delta))$, where $Y \neq g^{x_a z} \bmod p$.

Since the tuple $(m, y_a, \sigma = (Y, \alpha, \beta, \delta))$ is valid, both $g^\delta = \alpha y_a^h \bmod p$ and $(m)^\delta = \beta Y^h \bmod p$ hold. Certainly, the adversary A may use x_a and

the same random value r to generate another valid tuple $(m, y_a, \sigma' = (Y' = g^{x_a z}, \alpha, \beta, \delta'))$ as follows: $Y' = (m)^{x_a} \bmod p$, $\alpha = g^r \bmod p$, $\beta = (m)^r \bmod p$, $h' = H(y_a, m, Y', \alpha, \beta)$, and $\delta' = r + h' x_a \bmod q$.

Thus, $(m, y_a, \sigma' = (Y' = g^{x_a z}, \alpha, \beta, \delta'))$ is another valid tuple such that both $g^{\delta'} = \alpha y_a^{h'} \bmod p$ and $(m)^{\delta'} = \beta Y'^{h'} \bmod p$.

By Theorem 1, we know that if both $g^{\delta} = \alpha y_a^h \bmod p$ and $g^{\delta'} = \alpha y_a^{h'} \bmod p$ hold, the secret key x_a will be derived by $\log_g(y_a) = \frac{\delta - \delta'}{h - h'}$. It is a contradiction for the assumption of the difficulty of computing discrete logarithm. Therefore, we have $h = h'$ and $\delta = \delta'$. Since both $(m)^{\delta} = \beta Y^h \bmod p$ and $(m)^{\delta'} = \beta Y'^{h'} \bmod p$ hold, it is clear that $(Y/Y')^h = 1 \bmod p$. So we have $Y = Y'$ which is a contradiction for the $Y \neq g^{x_a z} \bmod p$ assumption. Therefore, the verifier can ensure that Y is equal to the Diffie-Hellman computation value $g^{x_a z} \bmod p$. □

5.2 Performance Analysis

The following notations are used to analyze the computational cost.

- T_{exp}: The time of executing a modular exponential operation.
- T_{mul}: The time of executing a modular multiplication operation.
- T_H: The time of executing a one-way hash function $H()$.

Note that the time of executing a modular addition operation is trivial in comparison with T_{exp}, T_{mul}, and T_H. In the following, we analyze the computational cost of our convinced DH computation scheme. For the issuing algorithm, the issuer requires $3T_{exp} + T_{mul} + T_H$ to compute $(Y, \alpha, \beta, \delta)$. For the verifying algorithm, the verifier requires $4T_{exp} + 2T_{mul} + T_H$ to validate $(Y, \alpha, \beta, \delta)$.

If the convinced DH computation scheme is embedded in the previously proposed group key protocols, it certainly requires more computational costs than the original protocol. However, the point is that the resulting GKA protocol is secure against malicious participant attacks and provides identifying malicious participants.

6 A Concrete Application

As mentioned in Section 1, the security of most GKA protocols is based on the related assumptions of the Diffie-Hellman problem. These Diffie-Hellman-based protocols cannot identify who malicious participant are, even if both authentication and key confirmation are involved in these protocols. They require multiple rounds to establish a common key, and each participant must compute the value of the Diffie-Hellman problem according to the received values in the previous round. For the adopted techniques, these protocols are classified into two categories: linear-round [7,8,9,14,16] and constant-round [10,11,12,13,15,17,18,19,20]. In which, these linear-round protocols are extended or modified from [7], while constant-round protocols are based on [11].

Our novel convinced DH computation scheme can be embedded in both linear-round and constant-round GKA protocols to provide the functionality of identifying malicious participants. In the following, we will present a concrete deployment on [7] to show the usage of our convinced DH computation scheme.

6.1 Review of Steiner et al.'s GKA Protocol

In [7], Steiner et al. proposed several linear-round group key agreement protocols. Here, we review the basic protocol (GDH.2). It consists of two stages: up-flow and broadcast. Without loss of generality, let $U = \{U_1, U_2, \ldots, U_n\}$ be the initial set of participants that want to generate a common key. U_1 initializes the up-flow stage and selects a random integer $x_1 \in Z_q^*$, then U_1 computes $g^{x_1} \bmod p$ and sends it to the next participant U_2.

Stage 1 (up-flow): Upon receiving the participant U_{i-1}'s messages, U_i selects a random integer $x_i \in Z_q^*$, and computes $\{g^{\prod(x_k|k\in[1,i]\wedge k\neq j)}|j \in [1,i]\}$ and $g^{x_1x_2\cdots x_i}$, then sends them to the next participant U_{i+1}.

Stage 2 (broadcast): When U_n receives the participant U_{n-1}'s messages, U_n selects a random integer $x_n \in Z_q^*$ and computes $\{g^{\prod(x_k|k\in[1,n]\wedge k\neq i)}|i \in [1,n]\}$, and then broadcasts them to all group participants. Finally, all participants may use their own secret x_i to compute the common key $g^{x_1x_2\cdots x_n}$.

6.2 Weakness and Enhancement of Steiner et al.'s GKA Protocol

In the following, we show that Steiner et al.'s group key agreement protocol cannot withstand malicious participant attack. For example, U_3 receives the set $\{g^{x_1}, g^{x_2}, g^{x_1x_2}\}$ from U_2 and forwards $\{g^{x_1x_2}, g^{x_1x_3}, g^{x_2x_3}, g^{x_1x_2x_3}\}$ to the next participant U_4. Assume that the malicious participant U_2 who wants to disrupt the group key establishment among honest participants. The malicious participant U_2 does not follow Stage 1 to compute the correct values $\{g^{x_1}, g^{x_2}, g^{x_1x_2}\}$ and replace them to send $\{g^{x_1}, g^{x_2}, R\}$ to U_3, where R is a random number. Thus, U_3 cannot find that U_2 has sent the wrong messages. Meanwhile, this wrong message will incur ripple-error computations of other following participants. Thus, all participants will obtain different group keys, respectively. The common key will not be constructed and the secure conference will not be held. Even if both authentication and key confirmation are involved in this protocol, honest participants cannot identify the malicious participant.

Here, we embed the convinced DH computation scheme in Steiner et al.'s group key agreement protocol to provide the functionality of identifying malicious participants. Upon receiving U_{i-1}'s i messages $(\{g^{\prod(x_k|k\in[1,i-1]\wedge k\neq j)}|j \in [1,i-1]\}, g^{x_1x_2\cdots x_{i-1}})$, U_i selects a random integer $x_i \in Z_q^*$ and computes $y_i = g^{x_i} \bmod p$. Without loss of generality, we denote these i messages as the set $\{g^{c_1}, g^{c_2}, \ldots, g^{c_i}\}$. Then, for each element $g^{c_k}(k = 1, 2, \ldots, i)$, U_i selects an random integer $r_k \in Z_q^*$ to compute and send the following values to U_{i+1}: $Y_k = (g^{c_k})^{x_i} \bmod p$, $\alpha_k = g^{r_k} \bmod p$, $\beta_k = (g^{c_k})^{r_k} \bmod p$ and $\delta_k = r_k + h_k x_i \bmod q$, where $h_k = H(g^{x_i}, g^{c_k}, Y_k, \alpha_k, \beta_k)$.

When U_{i+1} receives $(g^{c_k}, y_i, Y_k, \alpha_k, \beta_k, \delta_k)$ for $k = 1, 2, \ldots, i$, U_{i+1} checks whether both $g^{\delta_k} = \alpha_k y_i^{h_k} \bmod p$ and $(g^{c_k})^{\delta_k} = \beta_k Y_k^{h_k} \bmod p$ hold or not, where $h_k = H(g^{x_i}, g^{c_k}, Y_k, \alpha_k, \beta_k)$. Obviously, U_{i+1} can be convinced that U_i has computed and sent the correct messages.

Therefore, if our convinced DH computation scheme is involved in Steiner et al.'s group key agreement protocol, the enhancement may withstand and

identify the malicious participant. By space limitation, the complete security analysis of this enhancement is ignored here. It is clear that by Theorems 1 and 2, each participant can convinced the next participant that he/she has computed and sent correct messages. According to performance analysis mentioned in Subsection 5.2, it is clear that the enhancement will add some extra computational cost and messages. But, the point is that identifying malicious participants and fault tolerance will be achieved.

7 Conclusions

In this paper, we have proposed a new cryptographic mechanism called the convinced Diffie-Hellman (DH) computation scheme. We have defined the formal framework and security requirements for this new scheme. In the random oracle model and under the difficulty of computing discrete logarithm, we have shown that the proposed scheme is provably secure for two security requirements. To show the importance of the convinced DH computation scheme, one concrete deployment has been given. We embed the convinced DH computation scheme in Steiner et al.'s GKA protocol to provide the property of identifying malicious participants. For improving performance, the design of a convinced DH computation scheme with batch verification is an interesting future work. Due to the proposed convinced DH computation scheme has the convinced property, we will use this property into possible cooperative applications to provide robustness in the future.

Acknowledgements. This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC97-2221-E-018-010-MY3.

References

1. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
2. McCurley, K.S.: The discrete logarithm problem. In: Proceedings of Symposia in Applied Mathematics, pp. 49–74. AMS press (1990)
3. Maurer, U.M., Wolf, S.: Diffie-Hellman oracles. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 268–282. Springer, Heidelberg (1996)
4. Maurer, U.M., Wolf, S.: Diffie-Hellman, decision Diffie-Hellman, and discrete logarithms. In: Proc. IEEE international symposium on information theory, p. 327. IEEE press, Los Alamitos (1998)
5. Pfitzmann, B., Sadeghi, A.: Anonymous fingerprinting with direct non-repudiation. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 401–414. Springer, Heidelberg (2000)
6. Bao, F., Deng, R.H., Zhu, H.: Variations of Diffie-Hellman problem. In: Qing, S., Gollmann, D., Zhou, J. (eds.) ICICS 2003. LNCS, vol. 2836, pp. 301–312. Springer, Heidelberg (2003)
7. Steiner, M., Tsudik, G., Waidner, M.: Diffie-Hellman key distribution extended to group communication. In: CCS 1996, pp. 31–37. ACM press, New York (1996)

8. Steiner, M., Tsudik, G., Waidner, M.: CLIQUES: A new approach to group key agreement. In: ICDCS 1998, pp. 380–387. IEEE press, Los Alamitos (1998)
9. Steiner, M., Tsudik, G., Waidner, M.: Key agreement in dynamic peer groups. IEEE Trans. Par. Distrib. Systems 11(8), 769–780 (2000)
10. Horng, G.: An efficient and secure protocol for multi-party key establishment. The Computer Journal 44(5), 463–470 (2001)
11. Burmester, M., Desmedt, Y.: A secure and efficient conference key distribution system. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 275–286. Springer, Heidelberg (1995)
12. Burmester, M., Desmedt, Y.: A secure and scalable group key exchange system. Information Processing Letters 94(3), 137–143 (2005)
13. Tseng, Y.M.: A resource-constrained group key agreement protocol for imbalanced wireless networks. Computers & Security 26(4), 331–337 (2007)
14. Ateniese, G., Steiner, M., Tsudik, G.: New multiparty authentication services and key agreement protocols. IEEE J. Sel. Areas Communications 18(4), 628–639 (2000)
15. Boyd, C., Nieto, G.: Round-optimal contributory conference key agreement. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 161–174. Springer, Heidelberg (2002)
16. Bresson, E., Chevassut, O., Pointcheval, D.: Dynamic group diffie-hellman key exchange under standard assumptions. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 321–336. Springer, Heidelberg (2002)
17. Katz, J., Yung, M.: Scalable Protocols for Authenticated Group Key Exchange. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 110–125. Springer, Heidelberg (2003)
18. Wu, T.Y., Tseng, Y.M.: Comments on an ID-based authenticated group key agreement protocol with withstanding insider attacks. IEICE Trans. on Fundamentals of Electronics, Communications of Computer E92-A(10), 2638–2640 (2009)
19. Katz, J., Shin, J.S.: Modeling insider attacks on group key exchange protocols. In: CCS 2005, pp. 180–189. ACM press, New York (2005)
20. Bresson, E., Manulis, M.: Contributory group key exchange in the presence of malicious participants. IET Information Security 2(3), 85–93 (2008)
21. Tseng, Y.M.: A robust multi-party key agreement protocol resistant to malicious participants. The Computer Journal 48(4), 480–487 (2005)
22. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: CCS 1993, pp. 62–73. ACM press, New York (1993)
23. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. Journal of ACM 51(4), 557–594 (2004)
24. ElGamal, T.: A public-Key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31(4), 469–472 (1985)
25. Schnorr, C.P.: Efficient Signature Generation by Smart Cards. Journal of Cryptology 4(3), 161–174 (1991)
26. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996)
27. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. Journal of Cryptography 13(3), 361–396 (2000)

An Identifiable Yet Unlinkable Authentication System with Smart Cards for Multiple Services

Toru Nakamura[1], Shunsuke Inenaga[1], Daisuke Ikeda[1],
Kensuke Baba[2], and Hiroto Yasuura[1]

[1] Graduate School/Faculty of Information Science and Electrical Engineering,
Kyushu University
Moto'oka 744, Nishi-ku, Fukuoka, 819-0395, Japan
{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp,
daisuke@inf.kyushu-u.ac.jp
[2] Research and Development Division, Kyushu University Library
10-1, Hakozaki 6, Higashi-ku, Fukuoka, 812-8581, Japan
baba@lib.kyushu-u.ac.jp

Abstract. The purpose of this paper is to realize an authentication system which satisfies four requirements for security, privacy protection, and usability, that is, *impersonation resistance against insiders*, *personalization*, *unlinkability in multi-service environment*, and *memory efficiency*. The proposed system is the first system which satisfies all the properties. In the proposed system, transactions of a user within a single service can be linked (personalization), while transactions of a user among distinct services can not be linked (unlinkability in multi-service environment). The proposed system can be used with smart cards since the amount of memory required by the system does not depend on the number of services. First, this paper formalizes the property of unlinkability in multi-service environment, which has not been formalized in the literatures. Next, this paper extends an identification scheme with a pseudorandom function in order to realize an authentication system which satisfies all the requirements. This extension can be done with any identification scheme and any pseudorandom function. Finally, this paper shows an implementation with the Schnorr identification scheme and a collision-free hash function as an example of the proposed systems.

1 Introduction

With the increase of the number of services which a user would like to use, it is becoming more and more tedious for the user to establish and manage pairs of a user name (pseudonym) and a password of multiple services. Hence much attention is recently paid to authentication systems which enable users to use multiple services after they register at a registration manager only once. For example, single-sign-on systems, such as Shibboleth [2], OpenID [1], and so on, have been popular. In this paper, such a system is called *an authentication system in multi-service environment*.

The multi-service environment raises a new problem on privacy of users, that is, the daily activity of a user can be revealed from information in multiple service providers. Service providers usually maintain service logs of the transactions for the purpose of

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 236–251, 2010.

the detection of abuse, audit, and diagnosis of problems, and they can collect their log files and trace actions of a user from his/her transactions. This can be done if the same pseudonym is associated with the same user and is used for multiple service providers. In fact, a typical single-sign-on system is based on such an implementation, hence much more information in various service providers can be collected due to leakages of the service logs or illegal coalitions among multiple service providers. In order to solve the problem, authentication systems should have the property that it is difficult to determine whether multiple transactions in distinct service providers are related to the same user or not (*unlinkability in multi-service environment*). There are some authentication systems which satisfy unlinkability in multi-service environment, such as Janus [6], anonymous credentials [4], and authentication systems based on group signatures [5].

Authentication systems which satisfy unlinkability in multi-service environment can be classified according to the degree of unlinkability as follows.

- Transactions of a user can be linked within a service, while transactions of a user among distinct services. can not be linked.
- Transactions of a user can not be linked even within a service.

From the viewpoint of privacy protection, the systems with the latter property are superior to those with the former property. However, on the practical side, the systems with the latter property have some disadvantages. Indeed, without identification of each user, the purpose of service logs previously described cannot be achieved. Therefore, the system with the latter property cannot be applied to "personalized services", which customize and provide the contents according to a user's profile and preference. Examples of personalized services are personalized news and recommendation services. In the systems with the former property, service providers can identify each user (*Personalizasion*), hence they can maintain the service logs of their users and personalized service can be treated. In this paper, we focus on the systems with the former property.

Next, we consider how to maintain pairs of a pseudonym and a password. There are two ways on how to maintain pairs, that is, (1) doing by himself and (2) delegating the maintenance of the pairs to a trusted third party, such as a registration manager. We focus on the case (1) in this paper. In the case (1), some trusted devices, such as PCs and smart cards, are usually used for storing the pairs. A straightforward solution that satisfies both unlinkability in multi-service environment and personalization is that each user stores the table of the pairs of a pseudonym and a password for all service providers. In this solution, the amount of memory required by the system is proportional to the number of service providers. This solution would be efficient for systems with PCs as they have enough amount of memory. However, in this paper we are interested in situations where the portability of device of a user is indispensable, such as the use of ATM machines. Hence we consider a smart card as a device of a user. Notice that, since smart cards have much less memory than PCs, the above straightforward solution is unsuitable for smart cards when the number of service providers is considerably large. Therefore, it is important for any authentication system with smart cards to require as little amount of memory as possible in order to store pseudonyms and passwords (*Memory efficiency*).

The requirements for an authentication system considered in this paper are the following:

- *Personalization:* service providers can identify each user.
- *Unlinkability in multi-service environment*: it is difficult to determine whether two transactions among distinct service providers are the same user's or not.
- *Memory efficiency:* the amount of memory for pseudonyms and passwords does not depend on the number of service providers.
- *Impersonation resistance against insiders:* even if an adversary is a service provider, the adversary cannot impersonate a legitimate user.

In practical systems, the entities who try to impersonate a legitimate user are not only eavesdroppers but also malicious service providers. Therefore, authentication systems should have the property that an adversary cannot impersonate a legitimate user even if the adversary is a service provider.

We propose the first authentication system which satisfies all the requirements previously described. We note that there is no authentication system satisfies all of the requirements as far as we know. We show an extension of an identification scheme [7], which includes a key generating algorithm and an identification protocol, and the purpose of the extension is to realize the authentication system. The overview of our extended identification protocol is as follows:

- First, a user generates a pair of a pseudonym and a secret-key for each service provider from the corresponding *service ID* with pseudorandom functions [8].
- Next, the user and the service provider follow an identification protocol.

In order to evaluate our extended identification scheme, we define the above requirements based on the computational theory and we prove that our extended identification scheme satisfies all the requirements. To our knowledge, the definition of unlinkability in multi-service environment has not been formalized based on the computational theory, hence we show the first formalization of unlinkability in multi-service environment. The definition of impersonation resistance in this paper is based on the formalization of security of identification schemes in [7].

Related Work

Gabber *et al.* [6] proposed an authentication system, named Janus. In the Janus system, a user generates a pair of a pseudonym and a password for each service provider from his/her secret and the corresponding service ID with a cryptographic function. Hence the amount of memory does not depend on the number of service providers. The Janus system satisfies personarization, unlinkability in multi-service environment, and memory efficiency. However, the property of impersonation resistance was not much treated in [6]. Both Juang [10] and Hwang & Shiau [9] proposed authentication systems in multi-service environment with smart cards which satisfy memory efficiency. However, these systems cannot achieve unlinkability in multi-service environment. Liao and Wang [11] proposed the anonymous authentication system in multi-service environment with smart cards which have both memory efficiency and unlinkability in multi-service environment. However, service providers cannot identify each user in the system. Similarly, in anonymous credential systems [4] and in the systems based on group signatures [5], service providers cannot identify each user.

Organization

This paper is organized as follows. In Section 2 we recall the definition of identification schemes [7] and introduce its slight modification. In Section 3 we consider an extension of identification schemes to the case where there are multiple service providers. We also formalize the property of unlinkability in multi-service environment. Section 4 shows our proposed identification scheme which satisfies impersonation resistance, unlinkability, memory efficiency, and personalization. Section 5 describes an example of implementation of our authentication system based on the Schnorr identification scheme [12]. Section 6 concludes the paper.

2 Identification Scheme

In this paper, we show an extension of an identification scheme which realizes an authentication system which satisfies all the requirements, that is, impersonation resistance against insiders, personalization, unlinkability in multi-service environment, and memory efficiency. In this section, we first show the definition of identification schemes [7]. Next, we discuss the extension of the definition of identification schemes based on the equality of the outputs of protocols.

2.1 Definitions

An *interactive Turing machine* (ITM) is a multi-tape Turing machine with read-only input tapes, a read-and-write work tape, a write-only output tape, a pair of communication tapes, and a read-and-write switch tape consisting of a single cell. One communication tape is read-only and the other is write-only.

Two ITMs $\mathcal{A}$ and $\mathcal{B}$ are said to be linked if

- an input tape of $\mathcal{A}$ coincides with an input of $\mathcal{B}$,
- the read-only communication tape of $\mathcal{A}$ coincides with the write-only communication tape of $\mathcal{B}$, and vice versa, and
- the switch tape of $\mathcal{A}$ coincides with that of $\mathcal{B}$.

The shared input tape is called the *common input tape* of the two ITMs, while the other tapes are called an *auxiliary input tape*. A *joint computation* of two linked ITMs is a sequence of pairs of the local configurations (that is, the state, the contents of the tapes, and the positions of the heads) of the ITMs, where the configuration of one ITM is not modified when the configuration of the other ITM is modified, which is realized by the switch tape (if the content of the switch tape is 0, the configuration of the one ITM is modified, and otherwise that of the another one is modified). The output of a joint computation is the content of the output tape of one of the ITMs.

The output of a Turing machine $\mathcal{A}$ on an input x is denoted by $\mathcal{A}(x)$. We denote by $\langle \mathcal{A}, \mathcal{B} \rangle$ a joint computation of ITMs $\mathcal{A}$ and $\mathcal{B}$, and by $\langle \mathcal{A}(y), \mathcal{B}(z) \rangle(x)$ its output on a common input x, an auxiliary input y for $\mathcal{A}$, and an auxiliary input z for $\mathcal{B}$. We sometimes omit the brackets if the input tapes are blank. In the rest of this paper, we sometimes call a Turing machine $\mathcal{A}$ an "algorithm" $\mathcal{A}$, and a joint computation $\langle \mathcal{A}, \mathcal{B} \rangle$ a "protocol". If $\mathcal{A}$ is a probabilistic algorithm, $\mathcal{A}_r(x)$ denotes the output of $\mathcal{A}$ on an input x and random coins r. We denote by $p(n)$ denotes any polynomial of $n \in \mathbf{N}$.

Definition 1. *An* identification scheme *is a pair of a probabilistic polynomial-time algorithm $\mathcal{I}$ and a protocol $\langle \mathcal{P}, \mathcal{V} \rangle$ of two probabilistic polynomial-time ITMs such that:*

– Viability: *For any $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$, and any $s \in \{0,1\}^n$,*

$$\Pr[\langle \mathcal{P}(s), \mathcal{V} \rangle(\alpha, \mathcal{I}_s(\alpha)) = 1] = 1.$$

– Impersonation resistance against insiders: *For any pair $(\mathcal{B}', \mathcal{B}'')$ of probabilistic polynomial-time ITMs, any sufficiently large $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$, and any z,*

$$\Pr[\langle \mathcal{B}''(z, T), \mathcal{V} \rangle(\alpha, \mathcal{I}_S(\alpha)) = 1] < \frac{1}{p(n)},$$

where S is a random variable uniformly distributed over $\{0,1\}^n$ and T is a random variable describing the output of $\mathcal{B}'(z)$ after interacting with $\mathcal{P}(S)$, on common input $(\alpha, \mathcal{I}_S(\alpha))$, for polynomially many times.

Then, the string s is called a *secret-key*, the string α is called a *pseudonym*, the algorithm $\mathcal{I}$ is called a *verifying-key generating algorithm*, the output of $\mathcal{I}$ is called a *verifying-key*, and the protocol $\langle \mathcal{P}, \mathcal{V} \rangle$ is called an *identification protocol*.

2.2 Extension Based on Equality of Output of Protocols

In this section, we extend the identification scheme by the equality of the outputs of protocols. We also show the extended identification schemes which satisfies viability and impersonation resistance.

For any protocol $\langle \mathcal{A}, \mathcal{B} \rangle$ and any input x, it is easy to see that there exists a protocol $\langle \mathcal{A}', \mathcal{B}' \rangle$ such that

$$\langle \mathcal{A}, \mathcal{B} \rangle(x) = \langle \mathcal{A}'(x), \mathcal{B}'(x) \rangle.$$

In addition, it is easy to see that there exists a protocol $\langle \mathcal{A}'', \mathcal{B}'' \rangle$ such that

$$\langle \mathcal{A}'(x), \mathcal{B}'(x) \rangle = \langle \mathcal{A}''(x), \mathcal{B}'' \rangle.$$

The next lemma follows from the above arguments.

Lemma 1. *For any identification protocol $\langle \mathcal{P}, \mathcal{V} \rangle$, any $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$, and any $s \in \{0,1\}^n$, there exists a protocol $\langle \mathcal{P}', \mathcal{V}' \rangle$ such that*

$$\langle \mathcal{P}(s), \mathcal{V} \rangle(\alpha, \mathcal{I}_s(\alpha)) = \langle \mathcal{P}'(s, \alpha), \mathcal{V}' \rangle(\mathcal{I}_s(\alpha)).$$

For instance, the protocol $\langle \mathcal{P}', \mathcal{V}' \rangle$ can be constructed as follows:

1. $\mathcal{P}'$ is an ITM which reads α on the auxiliary input tape, writes α in the write-only communication tape, and then behaves in the same manner as $\mathcal{P}$.
2. $\mathcal{V}'$ is a modification of $\mathcal{V}$, which reads α on the read-only communication tape instead of reading α on the common input tape.

The modified version of identification protocol $\langle \mathcal{P}', \mathcal{V}' \rangle$ is called the *extended identification protocol* w.r.t. $\langle \mathcal{P}, \mathcal{V} \rangle$.

Lemma 2. *If $(\mathcal{I}, \langle \mathcal{P}, \mathcal{V} \rangle)$ is an identification scheme and $\langle \mathcal{P}', \mathcal{V}' \rangle$ is the extended identification protocol w.r.t. $\langle \mathcal{P}, \mathcal{V} \rangle$, the* extended identification scheme *$(\mathcal{I}, \langle \mathcal{P}', \mathcal{V}' \rangle)$ satisfies the following property: for any pair $(\mathcal{B}', \mathcal{B}'')$ of probabilistic polynomial-time ITMs, any sufficiently large $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$, and any z,*

$$\Pr[\langle \mathcal{B}''(z, T, \alpha), \mathcal{V}' \rangle(\mathcal{I}_S(\alpha)) = 1] < \frac{1}{p(n)},$$

where S is a random variable uniformly distributed over $\{0,1\}^n$ and T is a random variable describing the output of $\mathcal{B}'(z)$ after interacting with $\mathcal{P}'(S, \alpha)$, on common input $(\mathcal{I}_S(\alpha))$, for polynomially times.

Proof. Assuming that there exists a pair $(\mathcal{C}', \mathcal{C}'')$ of probabilistic polynomial-time ITMs such that for some $\alpha' \in \{0,1\}^n$, some z', and some polynomial $q(n)$ of n,

$$\Pr[\langle \mathcal{C}''(z', T', \alpha), \mathcal{V}' \rangle(\mathcal{I}_{S'}(\alpha')) = 1] \geq \frac{1}{q(n)},$$

where S' is a random variable uniformly distributed over $\{0,1\}^n$ and T' is a random variable describing the output of $\mathcal{C}'(z')$ after interacting with $\mathcal{P}'(S', \alpha')$ on the common input $(\mathcal{I}_{S'}(\alpha'))$ for polynomially times. We can construct a pair $(\mathcal{D}', \mathcal{D}'')$ of probabilistic polynomial-time ITMs such that:

1. $\mathcal{D}'$ is a modification of $\mathcal{C}'$, which reads α on the read-only communication tape instead of reading α.
2. $\mathcal{D}''$ is an ITM which skips writing α on the write-only communication tape, and then behaves in the same manner as $\mathcal{C}''$.

Then the distribution of the random variable T'', which describes the output of $\mathcal{D}'$ after interacting with $\mathcal{P}(S')$, equals the distribution of T'. According to previous 1 and 2, the pair of $\mathcal{D}'$ and $\mathcal{D}''$ satisfies the following property:

$$\Pr[\langle \mathcal{D}''(z', T'), \mathcal{V} \rangle(\alpha, \mathcal{I}_{S'}(\alpha')) = 1] \geq \frac{1}{q(n)}.$$

This is contradictory to Definition 1. □

The next theorem follows from Lemma 1 and Lemma 2:

Theorem 1. *If $(\mathcal{I}, \langle \mathcal{P}, \mathcal{V} \rangle)$ is an identification scheme and $\langle \mathcal{P}', \mathcal{V}' \rangle$ is the extended identification protocol w.r.t. $\langle \mathcal{P}, \mathcal{V} \rangle$, the extended identification scheme $(\mathcal{I}, \langle \mathcal{P}', \mathcal{V}' \rangle)$ satisfies the following property:*

- Viability*: for any $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$, and any $s \in \{0,1\}^n$,*

$$\Pr[\langle \mathcal{P}'(s, \alpha), \mathcal{V}' \rangle(\mathcal{I}_s(\alpha)) = 1] = 1.$$

- Impersonation resistance against insiders*: for any pair $(\mathcal{B}', \mathcal{B}'')$ of probabilistic polynomial-time ITMs, any sufficiently large $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$, and any z,*

$$\Pr[\langle \mathcal{B}''(z, T), \mathcal{V}' \rangle(\mathcal{I}_S(\alpha)) = 1] < \frac{1}{p(n)},$$

where S is a random variable uniformly distributed over $\{0,1\}^n$ and T is a random variable describing the output of $\mathcal{B}'(z)$ after interacting with $\mathcal{P}'(S, \alpha)$ on common input $\mathcal{I}_S(\alpha)$, for polynomially many times.

3 Extension of Identification Scheme for Multi-service Environment and Unlinkability in Multi-service Environment

In this section, we define identification schemes in multi-service environment by extending identification schemes of Definition 1. The key is the use of a set of functions that map strings to strings. We also formalize the property of *unlinkability in multi-service environment*.

3.1 Extension of Identification Scheme for Multi-service Environment

In order to describe identification schemes in multi-service environment, we introduce *user IDs* and *service IDs*, which are n-bit strings corresponding uniquely to users and service providers, respectively. We consider a set of functions that map strings which indicate service IDs to strings which indicate pseudonyms or secret-keys. For ease of explanation, we consider only length-preserving functions. Let F be a set of functions that map n-bit strings to n-bit strings, that is, $F = \{f_x : \{0,1\}^n \to \{0,1\}^n\}_{x\in\{0,1\}^n}$, where $x \in \{0,1\}^n$ indicates a user ID.

Let F and G be sets of functions mapping n-bit strings to n-bit strings. For any user ID a and any service ID b, $f_a(b)$ and $g_a(b)$ denote the secret-key and the pseudonym corresponding to the pair (a, b), respectively.

Then, we define *identification schemes in multi-service environment*, which is a quadruplet of a verifying-key generating algorithm $\mathcal{I}$, an identification protocol $\langle \mathcal{P}, \mathcal{V} \rangle$, sets F, and G of functions. An identification scheme in multi-service environment is constructed by replacing a secret-key s and a pseudonym α in Definition 1 with $f_a(b)$ and $g_a(b)$, respectively. An identification scheme in multi-service environment clearly satisfies the property of viability in Definition 1.

3.2 Unlinkability in Multi-service Environment

We define the property concerning privacy protection, which is called *unlinkability in multi-service environment*. Informally, this property means that it is difficult for any adversaries to determine whether two pseudonyms (and secret-keys) for distinct service IDs are generated from the same user ID or not. We define this property as follows:

Definition 2. *An identification scheme in multi-service environment* $(\mathcal{I}, \langle \mathcal{P}, \mathcal{V} \rangle, F, G)$ *has* unlinkability in multi-service environment *if for any probabilistic polynomial-time algorithm* $\mathcal{A}$*, any sufficiently large* $n \in \mathbf{N}$*, and any* $b \neq b' \in \{0,1\}^n$*,*

$$\Pr[\mathcal{A}(g_U(b), g_U(b')) = 1] - \Pr[\mathcal{A}(g_U(b), g_W(b'))] = 1| < \frac{1}{p(n)}$$

and

$$|\Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_{f_U(b')}(g_U(b'))) = 1] - \Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_{f_W(b')}(g_W(b'))) = 1]| < \frac{1}{p(n)},$$

where U *and* W *are random variables independently and uniformly distributed over* $\{0,1\}^n$.

As an example of "linkable" schemes, we consider an identification scheme in multi-service environment in which the same secret-key and pseudonym (we assume they are unique for each user ID) are used for all the service providers. That is, we assume that for any a, f_a and g_a are functions which output the same string on any input b, that is, for any $a \in \{0,1\}^n$ and any $b, b' \in \{0,1\}^n$, $f_a(b) = f_a(b')$ and $g_a(b) = g_a(b')$. In this scheme, it is trivial to check whether or not two pseudonyms for distinct service providers are related to the same user. If an algorithm $\mathcal{A}'$ outputs 1 if the first input equals the second input, and outputs 0 otherwise, it then holds that $\Pr[\mathcal{A}'(g_U(b), g_U(b')) = 1] = 1$ and $\Pr[\mathcal{A}'(g_U(b), g_W(b')) = 1] < 1/p(n)$. Hence this scheme does not have unlinkability in multi-service environment.

4 Identification Scheme Achieving Impersonation Resistance, Unlinkability, Memory Efficiency, and Personalization

In this section, we propose an identification scheme in multi-service environment which satisfies impersonation resistance against insiders, unlinkability in multi-service environment, memory efficiency on auxiliary input tape, and personalization by using an identification scheme and pseudorandom functions [8].

4.1 Proposed Scheme

We explain the overview of our proposed scheme. Assume that each user stores two functions to generate his/her pseudonyms and secret-key. First, after receiving a service ID, a user generates the pair of the pseudonym and the secret-key with the service ID and his/her functions. Next, the user and the corresponding service provider follow an identification protocol. In order to evaluate our scheme, we further modify the definition of identification schemes.

Extension of Identification Scheme for Construction of Our Scheme. For any function f, let $\langle f \rangle$ be the description of an algorithm which on an input x returns $f(x)$, and we assume any Turing machine can execute the algorithm which compute f if the machine is given the description $\langle f \rangle$. If $\langle \mathcal{P}, \mathcal{V} \rangle$ is an identification protocol and $\langle \mathcal{P}', \mathcal{V}' \rangle$ is the extended identification protocol w.r.t. $\langle \mathcal{P}, \mathcal{V} \rangle$, *the re-extended identification protocol* $\langle \mathcal{P}'', \mathcal{V}' \rangle$ w.r.t. $\langle \mathcal{P}, \mathcal{V} \rangle$ is constructed as follows:

- $\mathcal{P}''$ is an ITM which first reads $\langle f_a \rangle$ and $\langle g_a \rangle$ on the auxiliary input tape. After reading b on the common input tape, $\mathcal{P}''$ computes $f_a(b)$ and $g_a(b)$. Next, $\mathcal{P}''$ reads $f_a(b)$ and $g_a(b)$ instead of reading the auxiliary input s, α of $\mathcal{P}'$, and then behaves in the same manner as $\mathcal{P}'$.

Our proposed scheme is a quadruplet of a verifying-key generating algorithm $\mathcal{I}$, a re-extended identification protocol $\langle \mathcal{P}'', \mathcal{V}' \rangle$, pseudorandom functions F, and G. In what follows, we show that our identification scheme satisfies impersonation resistance against insiders, unlinkability in multi-service environment, memory efficiency on auxiliary input tape, and personalization.

Pseudorandom Functions. A *pseudorandom function*, which is a multi-set of functions that map strings to strings, cannot be distinguished from a truly random function.

An *oracle machine* is a Turing machine with an additional tape, called the oracle tape, and two special states, called oracle invocation and oracle appeared. For configurations with states different from oracle invocation, the next configuration is defined as usual. Let γ be a configuration in which the state is oracle invocation, the oracle is a function f, and the contents of the oracle tape is q. Then the configuration following γ is identical to γ, except that the state is oracle appeared, and the content of the oracle tape is $f(q)$. For any oracle machine $\mathcal{M}$ and function f, let $\mathcal{M}^f$ denote the output of $\mathcal{M}$ when given access to the oracle f. The string q is called *$\mathcal{M}$'s query* and $f(q)$ is called the *oracle reply*.

Definition 3. *A multi-set $F = \{f_x : \{0,1\}^n \to \{0,1\}^n\}_{x\in\{0,1\}^n}$ is called a* pseudorandom function*, if for any probabilistic polynomial-time oracle machine M, and any sufficiently large $n \in \mathbf{N}$,*

$$|\Pr[\mathcal{M}^{f_U}(1^n) = 1] - \Pr[\mathcal{M}^H(1^n) = 1]| < \frac{1}{p(n)},$$

where U is a random variable uniformly distributed over $\{0,1\}^n$ and H is a random variable uniformly distributed over all functions from $\{0,1\}^n$ to $\{0,1\}^n$.

The following three lemmas are used to prove the impersonation resistance and unlinkability in multi-service environment of our identification scheme. The next lemma follows from Definition 3.

Lemma 3. *For any pseudorandom functions F, any $b \in \{0,1\}^n$, any probabilistic polynomial-time algorithm $\mathcal{A}$, and any $x \in \{0,1\}^n$,*

$$|\Pr[\mathcal{A}(f_U(b), x) = 1] - \Pr[\mathcal{A}(W, x) = 1]| < \frac{1}{p(n)}$$

where U and W are random variables independently and uniformly distributed over $\{0,1\}^n$.

Proof. According to Definition 3, the oracle reply which is given by the random variable H distributed over all functions on any query is obviously a random variable uniformly distributed over $\{0,1\}^n$. Assuming for contrary that there exists a probabilistic polynomial-time algorithm $\mathcal{A}'$ such that for some $x' \in \{0,1\}^n$ and some polynomial $q(n)$ of n,

$$|\Pr[\mathcal{A}'(f_U(b'), x') = 1] - \Pr[\mathcal{A}'(W, x') = 1]| \geq \frac{1}{q(n)}.$$

Let $\mathcal{M}'$ be a probabilistic polynomial-time oracle machine which receives the oracle reply $f_U(b')$ on a query b' and then invokes $\mathcal{A}'$ on inputs $f_U(b')$ and x'. Then we have that

$$|\Pr[\mathcal{M}'^{f_U}(1^n) = 1] - \Pr[\mathcal{M}'^{H}(1^n) = 1]| \geq \frac{1}{q(n)},$$

which contradicts Definition 3 of pseudorandom functions. □

The following lemma can be shown similarly to Lemma 3.

Lemma 4. *For any pseudorandom function F, any $b \in \{0,1\}^n$, any probabilistic polynomial-time algorithm $\mathcal{A}, \mathcal{B}$, and any $x \in \{0,1\}^n$,*

$$|\Pr[\mathcal{A}(\mathcal{B}(f_U(b), x)) = 1] - \Pr[\mathcal{A}(\mathcal{B}(W, x)) = 1]| < \frac{1}{p(n)},$$

where U and W are random variables independently and uniformly distributed over $\{0,1\}^n$.

The following lemma can be shown similarly to Lemma 4 since any joint computation can be simulated by a probabilistic polynomial-time algorithm.

Lemma 5. *For any pseudorandom functions F and G, any $b \in \{0,1\}^n$, any probabilistic polynomial-time algorithm $\mathcal{A}$, any protocol $\langle \mathcal{B}, \mathcal{C} \rangle$ of probabilistic polynomial-time ITMs, and any $x \in \{0,1\}^n$,*

$$|\Pr[\mathcal{A}(\langle \mathcal{B}(f_U(b), x), \mathcal{C} \rangle(g_U(b), y)) = 1] - \Pr[\mathcal{A}(\langle \mathcal{B}(W, x), \mathcal{C} \rangle(X, y)) = 1]| < \frac{1}{p(n)},$$

where U, W, and X are random variables independently and uniformly distributed over $\{0,1\}^n$.

4.2 Evaluation of Impersonation Resistance

In this section, we show that our proposed scheme in multi-service environment using pseudorandom functions as F and G satisfies impersonation resistance against insiders.

First, we prove that an identification scheme in multi-service environment with pseudorandom functions has impersonation resistance against insiders.

Theorem 2. *For any identification scheme in multi-service environment $(\mathcal{I}, \langle \mathcal{P}, \mathcal{V} \rangle, F, G)$ such that F and G are pseudorandom functions, any pair $(\mathcal{B}', \mathcal{B}'')$ of probabilistic polynomial-time ITMs, any sufficiently large $n \in \mathbf{N}$, any $b \in \{0,1\}^n$, and any z,*

$$\Pr[\langle \mathcal{B}''(z, T'), \mathcal{V} \rangle(g_U(b), \mathcal{I}_{f_U(b)}(g_U(b))) = 1] < \frac{1}{p(n)},$$

where U is a random variable uniformly distributed over $\{0,1\}^n$ and T' is a random variable describing the output of $\mathcal{B}'(z)$ after interacting with $\mathcal{P}(f_U(b))$, on common input $(g_U(b), \mathcal{I}_{f_U(b)}(g_U(b)))$, for polynomially many times.

Proof. For any probabilistic algorithm $\mathcal{A}$, there exists a deterministic algorithm $\mathcal{A}'$ that outputs $\mathcal{A}'(r, x) = \mathcal{A}_r(x)$ on input x and random coins r. According to Lemma 4 and Lemma 5, it holds that for any probabilistic polynomial-time algorithm $\mathcal{A}$ and any $b \in \{0,1\}^n$,

$$|\Pr[\mathcal{A}(\langle \mathcal{P}(f_U(b)), \mathcal{B}' \rangle(g_U(b), \mathcal{I}_{f_U(b)}(g_U(b)))) = 1] - \Pr[\mathcal{A}(\langle \mathcal{P}(W), \mathcal{B}' \rangle(g_U(b), \mathcal{I}_W(g_U(b)))) = 1]| < \frac{1}{p(n)},$$

where U and W are random variables uniformly and independently distributed over $\{0,1\}^n$. Therefore, it holds that

$$|\Pr[\langle \mathcal{B}''(z,T'),\mathcal{V}\rangle(g_U(b),\mathcal{I}_{f_U(b)}(g_U(b)))=1] - \Pr[\langle \mathcal{B}''(z,T),V\rangle(g_U(b),\mathcal{I}_W(g_U(b)))=1]| < \frac{1}{p(n)},$$

where $T = \langle \mathcal{P}(W),\mathcal{B}'\rangle(g_U(b),\mathcal{I}_W(g_U(b)))$ and $T' = \langle \mathcal{P}(f_U(b)),\mathcal{B}'\rangle(g_U(b),\mathcal{I}_{f_U(b)}(g_U(b)))$. According to the definition of impersonation resistance against insiders in Definition 1,

$$\Pr[\langle \mathcal{B}''(z,T),V\rangle(g_U(b),\mathcal{I}_W(g_U(b)))=1] < \frac{1}{p(n)},$$

hence

$$\Pr[\langle \mathcal{B}''(z,T'),V\rangle(g_U(b),\mathcal{I}_{f_U(b)}(g_U(b)))=1] < \frac{1}{p(n)}. \qquad \square$$

In the case where the common tape includes b in addition, it is can be proven that the scheme has impersonation resistance against insiders. The next theorem follows from Theorem 1 and Theorem 2:

Theorem 3. *If a pair $(\mathcal{I},\langle \mathcal{P},\mathcal{V}\rangle)$ is an identification scheme, then our proposed identification scheme, which is a quadruplet of $\mathcal{I}$, re-extended identification protocol $\langle \mathcal{P}'',\mathcal{V}'\rangle$ w.r.t. $\langle \mathcal{P},\mathcal{V}\rangle$ and pseudorandom functions F, and G, satisfies the following properties:*

- Viability*: for any $n \in \mathbf{N}$, any $a \in \{0,1\}^n$ and any $b \in \{0,1\}^n$,*

$$\Pr[\langle \mathcal{P}'(\langle f_a\rangle,\langle g_a\rangle),\mathcal{V}'\rangle(b,\mathcal{I}_{f_a(b)}(g_a(b)))=1]=1.$$

- Impersonation resistance against insiders*: for any pair $(\mathcal{B}',\mathcal{B}'')$ of probabilistic polynomial-time ITMs, any sufficiently large $n \in \mathbf{N}$, any $b \in \{0,1\}^n$ and any z,*

$$\Pr[\langle \mathcal{B}''(z,T'),\mathcal{V}'\rangle(b,\mathcal{I}_{f_U(b)}(g_U(b)))=1] < \frac{1}{p(n)},$$

where U is a random variable uniformly distributed over $\{0,1\}^n$ and T' is a random variable describing the output of $\mathcal{B}'(z)$ after interacting with $\mathcal{P}'(\langle f_U\rangle,\langle g_U\rangle)$, on common input b and $\mathcal{I}_{f_U(b)}(g_U(b))$, for polynomially many times.

4.3 Evaluation of Unlinkability in Multi-service Environment

In this section, we prove that our proposed identification schemes satisfies unlinkability in multi-service environment.

Theorem 4. *Our proposed identification scheme $(\mathcal{I},\langle \mathcal{P}'',\mathcal{V}'\rangle, F, G)$ has unlinkability in multi-service environment.*

Proof. According to Lemma 3,

$$|\Pr[\mathcal{A}(g_U(b), g_U(b')) = 1] - \Pr[\mathcal{A}(g_U(b), X) = 1]| < \frac{1}{p(n)} \tag{1}$$

and

$$|\Pr[\mathcal{A}(g_U(b), g_W(b')) = 1] - \Pr[\mathcal{A}(g_U(b), Y) = 1]| < \frac{1}{p(n)}, \tag{2}$$

where U, W, X, and Y are random variables independently and uniformly distributed over $\{0,1\}^n$. X and Y follow the same distribution, hence

$$|\Pr[\mathcal{A}(g_U(b), X) = 1] - \Pr[\mathcal{A}(g_U(b), Y) = 1]| < \frac{1}{p(n)}. \tag{3}$$

According to Inequalities (1), (2), and (3),

$$|\Pr[\mathcal{A}(g_U(b), g_U(b')) = 1] - \Pr[\mathcal{A}(g_U(b), g_W(b'))] = 1| < \frac{1}{p(n)}. \tag{4}$$

In a similar way, according to Lemma 4,

$$|\Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_{f_U(b')}(g_U(b'))) = 1] - \Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_X(Y)) = 1]| < \frac{1}{p(n)} \tag{5}$$

and

$$|\Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_{f_W(b')}(g_W(b'))) = 1] - \Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_Z(Q)) = 1]| < \frac{1}{p(n)}, \tag{6}$$

where U, W, X, Y, Z and Q are random variables independently and uniformly distributed over $\{0,1\}^n$. X and Z follow the same distribution and Y and Q follow the same distribution, hence

$$|\Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_X(Y)) = 1] - \Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_Z(Q)) = 1]| < \frac{1}{p(n)}. \tag{7}$$

According to Inequalities (5), (6), and (7),

$$|\Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_{f_U(b')}(g_U(b'))) = 1] - \Pr[\mathcal{A}(\mathcal{I}_{f_U(b)}(g_U(b)), \mathcal{I}_{f_W(b')}(g_W(b'))) = 1]| < \frac{1}{p(n)}.$$

□

4.4 Memory Efficiency on Auxiliary Input Tape

The auxiliary input tape of $\mathcal{P}''$ of our proposed identification scheme corresponds to the memory of each smart card of our authentication system. The memory efficiency on auxiliary input tape of identification schemes is defined as follows:

Definition 4. *An identification scheme in multi-service environment* $(\mathcal{I}, \langle \mathcal{P}, \mathcal{V} \rangle, F, G)$ *has* memory-efficiency on auxiliary input tape *if the length of the auxiliary input tape of* $\mathcal{P}$ *is independent of the number of service providers.*

There exist algorithms such that they compute f_a and g_a and the length of their descriptions is independent of the number of service providers. Therefore, we have the following theorem:

Theorem 5. *Our proposed identification scheme* $(\mathcal{I}, \langle \mathcal{P}'', \mathcal{V}' \rangle, F, G)$ *has memory-efficiency on auxiliary input tape.*

4.5 Personalization

The property of personalization is defined as follows:

Definition 5. *An identification scheme in multi-service environment* $(\mathcal{I}, \langle \mathcal{P}, \mathcal{V} \rangle, F, G)$ *has* personalization*, if for any sufficiently large* $n \in \mathbf{N}$ *and any* $b \in \{0,1\}^n$*,*

$$\Pr[f_U(b) = f_W(b)] < \frac{1}{p(n)} \text{ and } \Pr[g_U(b) = g_W(b)] < \frac{1}{p(n)}$$

where U *and* W *are uniformly and independently distributed over* $\{0,1\}^n$*.*

If F and G are pseudorandom functions, the scheme clearly has personalization because of the property of pseudorandom functions.

Theorem 6. *Our proposed identification scheme* $(\mathcal{I}, \langle \mathcal{P}'', \mathcal{V}' \rangle, F, G)$ *has personalization.*

5 An Example of Implementation

In this section, we show an example of implementation of our authentication system. The implementation is based on the Schnorr identification scheme [12], and uses a collision-free hash function instead of pseudorandom functions. We then estimate an overhead with respect to the run time of our scheme.

5.1 The Schnorr Identification Scheme

As an example of identification schemes, we introduce the scheme proposed by Schnorr [12]. The scheme is a three-move identification scheme based on the discrete logarithm problem. Bellare and Paracio [3] showed that the scheme is secure on the assumption that the one more inversion problem for discrete logarithm is hard in terms of an interactive computation.

The verifying-key generating algorithm in the Schnorr identification scheme outputs (p, q, g, X) on input $s \in \{0,1\}^k$ for a security parameter $k \in \mathbf{N}$, where p is a prime number such that $2^{k-1} \leq p < 2^k$, q is a prime divisor of $p-1$, g is a generator of a subgroup of $\mathbf{Z}_p^*$ of order q, and X is $g^s \bmod p$. In our system, (p, q, g) is regarded as common parameters and (p, q, g) can be computed independently of X. Hence the verifying-key generating algorithm can be divided into the algorithm $\mathcal{C}$, which outputs (p, q, g) on input 1^k, and the algorithm $\mathcal{I}'$, which outputs X on input s.

The Schnorr identification protocol is shown as follows and in Fig.1.

1. $\mathcal{P}$ chooses $y \in \mathbf{Z}_q$ randomly, computes $g^y \bmod p$, and send the result as Y to $\mathcal{V}$;
2. $\mathcal{V}$ chooses $c \in \mathbf{Z}_q$ randomly and sends c to $\mathcal{P}$;
3. $\mathcal{P}$ computes $y + cs \bmod q$ and sends the result as z to $\mathcal{V}$;
4. $\mathcal{V}$ outputs 1 if $g^z = YX^c \pmod p$, and 0 otherwise.

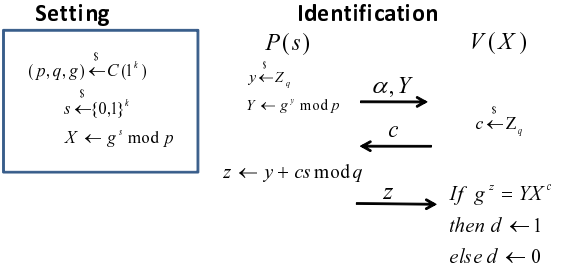


Fig. 1. The Schnorr identification scheme

5.2 The Implementation of Our Authentication System

Let $\{u_1, u_2, \ldots, u_\ell\}$ be the set of *users* and $\{s_1, s_2, \ldots, s_m\}$ the set of *service providers*. Each user secretly stores his/her user ID in his/her smart card. Let $\{a_1, a_2, \ldots, a_\ell\}$ be the set of user IDs. A user u_i is associated with his/her user ID a_i, and if $i \neq j$, then $a_i \neq a_j$. Each service provider is labelled by his/her service ID, which is the public identifier. Let $\{b_1, b_2, \ldots, b_m\}$ be the set of the service IDs. A service provider s_j is associated with his service ID b_j, and if $i \neq j$, then $b_i \neq b_j$.

We use a collision-free hash function in place of pseudorandom functions. More concretely, $h(0 \parallel a \parallel b)$ and $h(1 \parallel a \parallel b)$ are used as $f_a(b)$ and $g_a(b)$ in the system respectively, where h denotes a collision-free hash function and $\parallel$ denotes concatenation.

In our authentication system, there is a *manager* M, which sets up several parameters. First, we show the preparation procedure which is operated by M.

- **Startup:** M chooses a security parameter $k \in \mathbf{N}$, and computes (p, q, g) with the algorithm $\mathcal{C}$.
- **Registration of Users:** When a new user u_i requests to join in the system, M issues a smart card which stores $a_i \in \{0,1\}^k - \{a_1, a_2, \ldots a_{i-1}\}$ chosen randomly and (p, q, g) to u_i.
- **Registration of Services:** When a new service provider s_j requests to join in the system, M sends $b_j \in \{0,1\}^k - \{b_1, b_2, \ldots b_{i-1}\}$ chosen randomly and (p, q, g) to s_j. Then M computes pairs $(h(0 \parallel a_i \parallel b_j), h(1 \parallel a_i \parallel b_j))$ for all i, and sends pairs $(h(1 \parallel a_i \parallel b_j), g^{h(0 \| a_i \| b_j)} \bmod p)$ for all i to s_j.

Next, we show the identification protocol as follows and in Fig. 2.

1. u_i sends an authentication query to s_j.
2. s_j sends b_j to u_i.
3. u_i computes a pair $(h(0 \parallel a_i \parallel b_j), h(1 \parallel a_i \parallel b_j))$ and sends $h(1 \parallel a_i \parallel b_j)$ to s_j.
4. s_j specifies the corresponding $g^{h(0\|a_i\|b_j)} \bmod p$ from $h(1 \parallel a_i \parallel b_j)$.
5. u_i and s_j follow the Schnorr identification scheme.

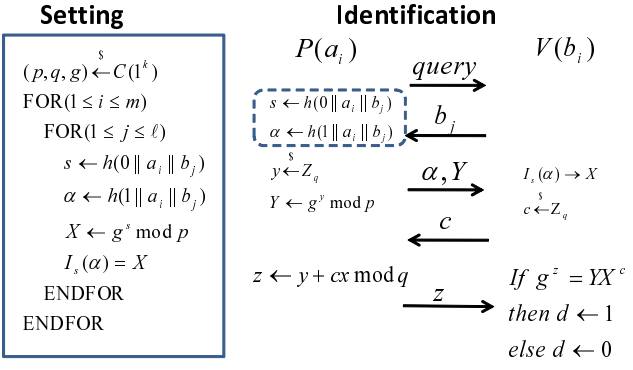


Fig. 2. Our identification scheme based on the Schnorr identification scheme

5.3 Discussion

A naive scheme realizing unlinkability in multi-service environment can be achieve by storing a user's secret-keys and pseudonyms, which are randomly chosen, in a table. In the naive scheme, the amount of memory which a user needs is proportional to the number of services. Using our scheme, the amount of memory does not depend on the number of services, however, two more hash computations are required compared to the naive scheme. Let $t_a(b) = h(0 \parallel a \parallel b)$ and $t'_a(b) = h(1 \parallel a \parallel b)$. Assuming that the sets $\{t_a\}_{a\in\{0,1\}^n}$ and $\{t'_a\}_{a\in\{0,1\}^n}$ are pseudorandom functions, the implementation of our authentication system satisfies impersonation resistance against insiders, unlinkability in multi-service environment, memory efficiency, and personalization.

6 Conclusions

In this paper we proposed an authentication system in multi-service environment which satisfies impersonation resistance, unlinkability in multi-service environment, memory efficiency, and personalization. Due to the use of pseudorandom functions, the memory requirement for each smart card is independent of the number of services. This is a remarkable advantage when a massive number of services utilize the system. We showed an example of our system based on the Schnorr identification scheme, in which pseudorandom functions are replaced with collision-free hash functions.

Our future work includes the following:

- Implementing our system with smart cards and a PC in order to measure the execution time and to compare it with that of other related authentication systems.
- A comparison of the circuit size of our implementation with a hash function and that of a naive method using a table of pairs of a pseudonym and a secret-key. We conjecture that as the number of service providers increase, our system will become more memory efficient than the naive method.

Acknowledgements

This work was in part supported by CREST-DVLSI of JST. We are grateful for their support.

References

1. OpenID, http://openid.net/
2. Shibboleth, http://shibboleth.internet2.edu/
3. Bellare, M., Palacio, A.: GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, p. 162. Springer, Heidelberg (2002)
4. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
5. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–270. Springer, Heidelberg (1991)
6. Gabber, E., Information, C., Gibbons, P.B., Matias, Y., Mayer, A.: How to make personalized web browsing simple, secure and anonymous. In: Luby, M., Rolim, J.D.P., Serna, M. (eds.) FC 1997. LNCS, vol. 1318, pp. 17–31. Springer, Heidelberg (1997)
7. Goldreich, O.: Foundations of Cryptography. Cambridge University Press, Cambridge (2001)
8. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. Journal of the ACM (JACM) 33(4), 792–807 (1986)
9. Hwang, R.J., Shiau, S.H.: Provably efficient authenticated key agreement protocol for multi-servers. The Computer Journal 50, 602–615 (2007)
10. Juang, W.S.: Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronics 50, 251–255 (2004)
11. Liao, Y.P., Wang, S.S.: A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer standards and interfaces 31(1), 24–29 (2009)
12. Schnorr, C.P.: Efficient signature generation by smart cards. Journal of Cryptology 4, 161–174 (1991)

Accelerating Video Identification by Skipping Queries with a Compact Metric Cache

Takaaki Aoki, Daisuke Ninomiya,
Arnoldo José Müller-Molina, and Takeshi Shinohara

Department of Artificial Intelligence, Kyushu Institute of Technology
Kawazu 680-4 Iizuka, 820-8502, Japan
e231001t@ai.kyutech.ac.jp,
shino@ai.kyutech.ac.jp

Abstract. Recently, the amount of multi-media data, such as movies, has been increasing rapidly. We often encounter situations which require fast and approximate retrieval of movies. A video is composed of multiple still images(frames). In this paper, we identify videos in real-time by performing retrieval of still images successively. When we use hierarchical similarity search indexes, results that are far away from a query are more costly to obtain than results that are close to a query. Far results are not useful for video identification. Nevertheless, it is important to know that no close results exist to correctly identify a video. The similarity between consecutive images is usually high because of the nature of video data. In this paper we propose a type of cache that exploits this fact by skipping queries that are likely not to have close results. We also employ an early termination strategy that avoids unnecessary distance computations to retrieve far results while preserving the quality of the video identification. By conducting experiments, we show that both methods provide considerable improvements. The proposed caching technique is able to skip up to 40% of the queries. The early termination strategy is able to reduce the number of distance computations to 0.5%. The combination of both techniques provides even greater gains.

1 Introduction

Nowadays, a large amount of video data is recorded and broadcasted worldwide. Examples range from security surveillance cameras to videos captured by web cameras. These types of videos are of particular interest because it is possible to perform actions in real-time depending on the content of the video. In the case of web-cameras, augmented reality applications are endless. For example, different facial expressions of the users could be recognized. After determining the mood of the user, overlays that reflect the situation could be added to enhance the users experience. In the case of surveillance cameras, given an example set of "dangerous situations" which breach security, the system could detect them in real-time if there is a security issue.

Since in general videos are composed of multiple still images, similarity search for videos can be carried out by performing retrieval of images for each of the frames of a video stream. Since this is a resource intensive task, it is necessary to reduce the load on the index as much as possible.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 252–262, 2010.

In this paper, we introduce a technique that can be applied to optimize indexes by employing historical query data. We exploit the fact that, in video data, the similarity between consecutive frames is usually high. Given a sequence $q_1, q_2, \ldots, q_n$ of query frames, we expect query q_{i-1} and q_i to be close to each other. If we know that q_{i-1} has an empty result, then it is likely that q_i will also have no results. Therefore, we can skip query q_i. We call this technique a *compact metric cache* (CMC). The cache only requires to know the result of the previous query q_{i-1}, and therefore it can be computed very efficiently. The searching method using cache by Falchi *et al.* [1] focuses on the queries which are likely to have some appropriate results, and it returns approximate results. On the other hand, our technique mainly works for queries which are not likely to have any results. Then our CMC also can work for queries which have close results, and it can return completely precise result. On these two points, our proposal is novel.

Depending on the domain it may not be necessary to perform retrieval of all frames of a query video to identify it correctly. For example, it may be enough to search only for the key frames used in the compression techniques, such as MPEG2. In this paper, we consider the case of searching each frame of a query video. This is specifically needed in the case of real-time video identification. It is not necessary for the real-time retrieval to consider the selection of key frames. Our approach can deal with raw video data, therefore we do not have to select key frames. As we describe in Section 4.6, we can achieve very fast identification without key frames based methods. Moreover, we may expect that the search for all frames of a query video can accomplish more precise identification because it can use any information such as frame position.

The purpose of our video identification application is to decide whether a given query video belongs to the database. If a frame of the query video has results within a certain amount of distance units, then we accept the match of the frame. Matches between too far frames are not meaningful and can be safety ignored without introducing incorrect identification.

We note that when the results are far from a query, it is likely that the index will perform more work than if the results are close to a query. This behavior can be observed in different similarity search indexes. We describe this in Section 4.1 in detail. As explained before, answers that are far away from a query are not useful to identify a video. On the other hand, it is important to know that there are no close answers to a given query to correctly report that the video does not belong to the database. We exploit this fact by employing an early termination heuristic [2] that reduces distance computations without impacting the accuracy of the results. We must gain precise answers for queries which have close results for correct identification, and these queries can be already efficiently retrieved by similarity search indexes. CMC can make the search of queries of this kind faster by shrinking the query radius, and it returns precise results. Furthermore, we can skip the search of queries which have only far or no results by CMC without introducing incorrect identification. Therefore, we can achieve efficient retrieval for all queries with CMC.

We measure the quality of our proposed techniques in a database that holds about 7 million frames extracted from about 2800 videos. We apply *NN range* queries that return a nearest neighbor object within a distance r. Our technique is able to skip about 45% of the frames of videos that do not belong to the database. In contrast, for videos

whose frames are close to objects in the database, the CMC skipping query ratios can go up to 1%. With CMC, we can reduce the number of distance computations to about 40% for queries that have only far results, and to about 94% for queries that have near results. Additionally, the early termination strategy is able to reduce the number of distance computation in up to two orders of magnitude. We sacrifice about 10% in frame accuracy with our methods, but we can achieve considerable performance gains without impacting video identification accuracy.

The rest of the paper is organized as follows. In Section 2 we describe relevant techniques. In Section 3 we describe our proposed approach. Finally in Section 4 we present the results of our experimental validation.

2 Background

There is a large number of similarity search indexes [2][3][4][5]. Our technique is related to the recently developed idea of metric caches [1].

2.1 Query History

Not many indexes, such as the *VQ-index* [6] and *VA-file* [7], make use of query history to enhance their performance.

Very recently, Falchi *et al.* proposed the *metric cache* [1], a mechanism that uses the properties of metric spaces to avoid the search of objects that are close to queries executed at some point in the past. Given a cache $\mathcal{C}$ placed in front of a similarity search index, the recent/frequently accessed queries and their respective answers are stored. If a query that has a close value in $\mathcal{C}$ arrives, then it is possible to return an approximate result directly.

As we mentioned before, close queries are already efficiently retrieved by similarity search indexes and therefore we consider other type of cache. Our approach deals with the far queries, which are very costly. To the best of our knowledge, this kind of cache technique is novel.

2.2 The Metric Spaces

Let $\mathcal{M} = (\mathcal{D}, d)$ be a *metric space* for a domain $\mathcal{D}$ of objects and $d : \mathcal{D} \times \mathcal{D} \rightarrow \mathbb{R}$, a total *distance function* that satisfies the *metric postulates* [2]: The most important property of them is the triangle inequality as described below:

$$\forall x, \forall y, \forall p \in \mathcal{D}, d(x, y) \leq d(x, p) + d(p, y).$$

Suppose a collection $X \subseteq \mathcal{D}$. A *k-nearest neighbor*(k-NN) query returns the k closest elements to the query object q. The set R of results is

$$\{R \subseteq X \mid |R| = k \wedge \forall x \in R, \forall y \in X - R : d(q, x) \leq d(q, y)\}.$$

We can also define a *k-NN range* query. For a range r, it returns the k closest elements within a distance r. In the case of $k = 1$ for a k-NN range query, we call this an *NN range* query.

While the initial query range of an NN query is infinite, that of an NN range query is a given query range r. If there are no objects within a distance r from a given query, this means that no answers exist. In this paper, we focus on NN range queries mainly.

2.3 Video Identification

To match videos, we take each still frame from a video and extract its features into a vector. Video similarity search indexes must deal with different video encodings, resolutions, and qualities. A series of normalization steps occur in the extraction process. These steps include monochrome transformation, thumbnail transformation, discrete Fourier transformation, normalization of brightness and so on. A more detailed overview of these techniques is presented in [8].

The similarity between still frames is computed by the L_1 distance. Each frame has an associated label that indicates to which video it belongs. At search time, we extract the still frames from a query video. Each frame is matched against the database, and we identify the video by majority of the detected labels. We prepare two types of query videos. The one is *positive data* which is videos that have some similar videos in the database. The other is *negative data* which is composed of videos that do not belong to the database. Therefore, negative data are not close to any videos in the database. We show the distance histogram of these query data in Section 4.3. We search all frames of the query video, and store the video label obtained by each answer frame. If the frequency of video label l exceeds some threshold, we assume the query video to be l. Otherwise, we decide that no match is found in the database. Experimentally, we have found that 3% is an appropriate threshold [8].

3 Proposed Approach

In this paper, we follow the hypothesis that hierarchical indexes can answer queries efficiently if the corresponding result is close to the query. Furthermore, the efficiency of the index decreases as the distance of the query to the result increases. In the context of video identification, results that are far from the query are useful to identify a video as negative. The exact value of such results is not important, what is important is that there are no close answers. In this section we describe a compact metric cache (*CMC*) that helps to avoid the search of costly queries, i.e., queries that do not have any associated results. We also employ a naive early termination heuristic to further improve performance.

3.1 CMC

We define a type of cache technique that avoids costly queries. We call this technique a *Compact Metric Cache* (*CMC* for short). We focus on NN range queries introduced in Section 2.2. CMC optimizes the method of searching queries by considering whether the previous query has a result or not. Our technique involves two major optimizations. The first optimization exploits empty results of the previous query. The second optimization works when the previous query had an associated result and it uses the query range information.

Previous Query Has an Empty Result: Let $search(q, r)$ be a procedure that returns an answer object to an NN range query for a query q with a range r. If there are no objects within r from q, it returns "$none$". Consider a sequence of queries $q_1, \ldots, q_n$ and

assume that $search(q_{i-1}, r) =$ "$none$". We call such a query with an empty result the *cache query*. Let c be a value that is much smaller than r. If the queries q_{i-1} and q_i are within distance c and if q_{i-1} is the cache query, we can skip q_i because it is likely that q_i has also an empty result. The answer for skipped queries is always "$none$". When we receive the query q_{i+1} we compare it to the cache query, q_{i-1}. If the distance between the cache query and q_{i+1} exceeds a threshold c, then we must execute $search(q_{i+1}, r)$. This simple scheme only requires an additional distance computation per query. The approach requires that objects are queried sequentially and that the distance between every consecutive queries is small.

In the following, we explain our proposal by using metric postulates. As described above, the cache query does not have an appropriate answer within a distance r:

$$\{\forall x \in \mathcal{D} | d(cache, x) < r\} = \emptyset.$$

Then, we assume $d(cache, q_i) < c$. For such cache query and q_i, by the triangle inequality,

$$d(q_i, x) \geq |d(cache, x) - d(cache, q_i)| > r - c.$$

Since query q_i has an empty result within range $r - c$, we can skip query q_i because q_i does not have answers with high probability. As c gets smaller, the precision of the results increases.

Previous Query Has a Result: Assume that q_i has an associated result. For the closest result $close$ of q_i obtained by an NN range query, if $d(close, q_{i+1}) < r$, we can shrink the query range r to $d(close, q_{i+1})$, because query q_{i+1} has at least one result within the shrunk query range. Objects that should be reviewed during the search are reduced by shrinking query range. Therefore, we can expect the cost to be low. This optimization provides small improvements and it does not affect the results at all.

Combination of Both Approaches: The mechanism of CMC is the combination of above two optimizations. We describe the algorithm of CMC in Algorithm 1. In Line 8 we shrink the query range (second optimization). In Line 11 we skip the query by using the first optimization. In Line 18 we reset the cache value.

3.2 Early Termination Heuristic

There are a number of early termination strategies [2][9][10]. In this paper we employ the naive early termination strategy in which the search is stopped prematurely after a certain number of distance computations f has been calculated. In practice, the threshold f can be obtained experimentally from a sample set of data.

4 Experiments

In this section we verify the effect of our proposed methods introduced in Section 3. To perform successive approximate retrieval of images, we employ a Hilbert R-Tree [11]

Algorithm 1. CMC

INPUT: r: search range, c: threshold for CMC ($c < r$), $q_1, \ldots, q_n$: a sequence of queries
OUTPUT: a sequence of results for each queries

```
close ← search(q_1, r) /* search(q, r): an NN range query for a query q with a range r */
output close
if close = "none" then
    cache ← q_1
end if
for i = 2 to n do
    if close ≠ "none" then
        r' ← min(r, d(close, q_i))    /* shrink of query range */
    else if d(cache, q_i) < c then
        output "none"
        continue    /* skip query */
    else
        r' ← r
    end if
    close ← search(q_i, r')
    output close
    if close = "none" then
        cache ← q_i
    end if
end for
```

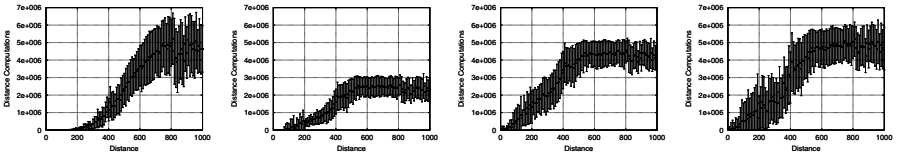
that stores embedded objects [12] which are projected into lower dimension by SimpleMap [13]. First we study the relation of the cost and distances of queries to their nearest neighbor on R-Tree and other three indexes. Then, we proceed to study the performance of our CMC method and the impact of the early termination strategies in video identification. Our dataset consists of 7 million images that are extracted from about 2800 videos. The videos are television commercials.

4.1 Comparison of R-Tree and Other Indexes

We compare our R-tree with other representative indexes for similarity search. We exploit *SAT* [14], *GHT* [15][16] and *LCluster* [17] methods. We apply 10000 as a partition size of the LCluster.

We prepare two types of query sets. *Positive data* is similar to the objects stored in the database. The other type of data is far from the database, and it is called *negative data*. In this paper, we have two sets of positive data queries. The first set *(close)* comprises queries with very small perturbation. The second set *(far)* is much more distorted. The close dataset contains slightly perturbed queries and the far set contains more modification. All the queries have been randomly perturbed with noise.

In this experiment we randomly select 10000 query objects from our dataset, then perform nearest neighbor queries. Figure 1 shows the results of each index. The x axis shows the distance of the closest result to the query and the y axis shows the number of distance computations involved in the calculation of each result. We can see that SAT performs much better than other three indexes in general. On the other hand, the cost



(a) R-tree (b) SAT (c) GHT (d) LCluster

Fig. 1. The Relation between Cost and Distance of the Result to the Query on Four Indexes. (The Cost Increases as the Results Get Farther from the Query on All Indexes).

of R-tree is lower than any other indexes while the value of the distance ranges from 0 to 300. Since we are primarily interested in searching for objects that are close to the query, the R-Tree fits our purposes.

Since the cost increases as the results get farther from the query on all indexes, the retrieval of negative data need much more cost than positive data. Negative data does not have any similar videos in the database, then it is not useful for video identification. Indexes should eliminate the search of negative data, but in general we cannot recognize whether the query is positive data or negative data before the retrieval of it. Therefore, we attempt to improve the efficiency of the process of video identification with the early termination heuristic because it is likely that the query is negative data if there are no proper results after a certain number of distance computations f has been passed.

4.2 The Criteria of Evaluation

Now, we call the nearest neighbor range search that does not use CMC or the early termination strategy the *usual method*.

We define the criterion to investigate the effect of our proposed approaches. We use the *improvement in efficiency* criteria [2] : $IE = \frac{cost(Q)}{cost^A(Q)}$ where $cost(Q)$ denotes the cost of the query set Q on R-tree by the usual method and $cost^A(Q)$ denotes the cost of Q on R-tree by our proposed methods. In this paper, the cost is the number of distance computations performed. We evaluate our methods on NN range queries which are introduced in Section 2.2.

We now define the criteria to inquire the error rate of our proposed techniques. CMC and the early termination heuristic may return an answer that differs from the one obtained by the usual method. Let b_1 be the number of such errors. The *frame error* is defined as $b_1/|Q|$ for a set of query frames Q. Also, our proposed techniques may incorrectly identify a video. On positive data, we compare the answer video obtained by our proposed techniques with the one of the usual method. Because all positive data certainly have an answer video by the usual method. Let b_2 be the number of videos identified falsely, the *video identification error* is defined as $b_2/|R|$ for a set of query videos R. On the other hand, we expect negative data not to have an answer video. Therefore, we do not define the video identification error for negative data.

The *frame skip percentage* reflects the ratio of queries that were skipped by CMC. Let b_3 be the number of query frames skipped by CMC, the frame skip percentage is defined as $b_3/|Q|$.

4.3 Query Range Selection

We need to determine that negative data do not belong to the database. The query data for positive (close, far) and negative consist of around 20000 frames extracted from about 30 videos respectively. The histogram of the distance of three query sets to their nearest neighbor object is described in Figure 2. The x axis shows the distance of the closest result to each query frame. From this graph, we select the query ranges used by an NN range query on the experiments. We select a value that clearly divides positive data from negative data. By referring to Figure 2, we determine 400 and 500 as the query ranges.

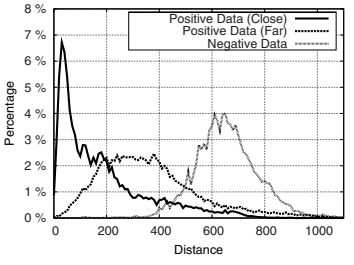


Fig. 2. Histogram of the Distance of the Closest Result to Each Query

If the query range is too small, no objects are obtained by the retrieval process, so we cannot identify the videos. In contrast, if query range is too large, most queries can find results. Nevertheless, we know that if a query does not have any associated results, it is costlier than one that has close results by referring to Figure 1. Since results that are far away from the query are not useful for video identification, an excessively large query range is meaningless.

4.4 Validation of CMC

We validate the effect of CMC which is introduced in Section 3. We change the value of c from 20 to 140 and study the behavior of the R-tree.

Figures 3 and 4 show the result of CMC for positive data (close) and negative data. As c gets bigger, the frame error, IE and frame skip percentage also increase. These three criteria for positive data (far) are slightly bigger than for positive data (close). The frame error is less than 0.1% for all values of c. Since negative data is likely not to have results, queries are more often skipped by CMC than positive data. All the measurements except video identification error are larger on negative data. In this experiment, CMC produces no video identification error for positive data (far and close).

When the query range is 400, negative data tends not to have results. If there are no associated results, CMC does not affect the frame error measurably. Therefore, frame error for negative data is lower on range 400 because it is likely to get empty results. When the range is 500, the frame error does increase because the number of non-empty results for negative data increases. In the case of positive data (close), it is also likely to have an empty result when the range is 400. Therefore, CMC skipped more queries.

4.5 Validation of the Early Termination Heuristic

Now, we validate the early termination heuristic. We study the behavior of the R-tree as f increases from 10000 to 1000000.

The early termination heuristic shows significant improvements in Figure 5 for positive data (close) and negative data. As f grows, the results become more precise and

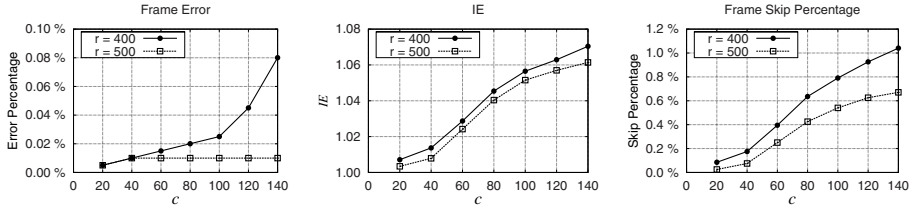


Fig. 3. Frame Error, IE and Frame Skip Percentage of Positive Data (Close) (CMC)

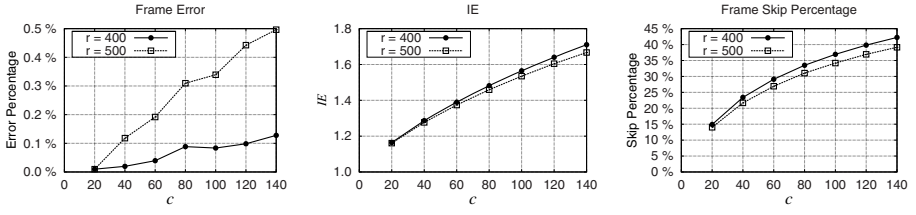


Fig. 4. Frame Error, IE and Frame Skip Percentage of Negative Data (CMC)

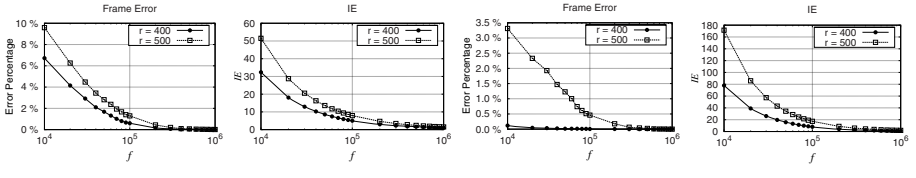
both the frame error and IE are reduced. These two criteria for positive data (far) are slightly bigger than for positive data (close). The video identification error for positive data (far and close) is nothing.

For the three query sets, the frame error and IE are lower on range 400. One of the reasons of this is the fact that for the usual method on range 400 many queries have empty results especially on negative data.

The early termination heuristic can substantially reduce the number of distance computations, but it is likely to return an incorrect result, especially on positive data. In the case of negative data, it achieves much bigger IE in spite of lower frame error than positive data. This is also by the fact that negative data is very likely to return empty results.

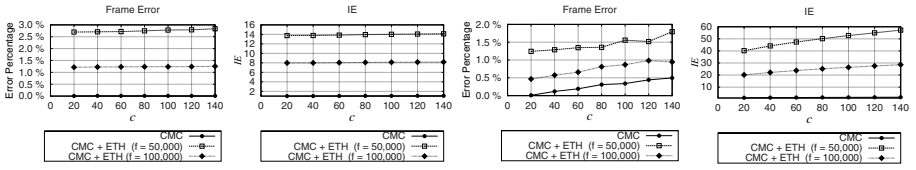
4.6 Validation of CMC + Early Termination Heuristic

Now, we validate the combination of CMC and the early termination heuristic. In this experiment, we use 500 as the query range, then apply 50000 and 100000 as the threshold f for the early termination heuristic. We also change the value of c for CMC from 20 to 140.



(a) Positive Data (Close) (b) Negative Data

Fig. 5. Frame Error and IE (Early Termination Heuristic)



(a) Positive Data (Close) (b) Negative Data

Fig. 6. Frame Error and IE (CMC + Early Termination Heuristic)

Figure 6 shows the results. The video identification error for positive data (close) is nothing. We can see that both techniques combined will produce greater gains than if used independently. This is because the early termination heuristic is likely to find an empty result. This in turn helps the CMC algorithm to skip even more queries. If we compare IE when $c = 100$, $f = 100000$ of Figures 4, 5 (b) and 6 (b) we can see that the combination of CMC (*IE*: 1.5) and the early termination heuristic (*IE*: 17) produce greater gains (*IE*: 26) without affecting considerably frame error.

We show the number of frames which are processed per second in Table 1. Our system can identify the query video in real-time by using the combination of CMC with the early termination heuristic (E.T.H) because the number of processed frames exceeds 30 which are the number of images contained in general video data per second.

Table 1. The Number of Processed Images per Second

Method	Positive Data (Close)	Negative Data
Usual	20.77	3.33
CMC + E.T.H (f = 50,000)	241.42	219.04
CMC + E.T.H (f = 100,000)	146.44	109.13

5 Conclusions

In this paper we presented a compact metric cache CMC that helps to avoid costly queries on the process of identification of video data. We experimentally demonstrated that by combining this cache with an early termination heuristic, it is possible to obtain improvements of two orders of magnitude over an unmodified index. Our compact metric cache can be used in searches of sequences of objects that are close to each other.

On all experiments in this paper, our proposed approaches obtained greater precision and IE on negative data than positive data. This is because negative data is likely to have no answers. Indexes that do not apply our proposed approaches perform retrieval for far query at a high cost.

Our proposed methods reduce the cost of retrieval process greatly, but introduce small errors. In the future, we would like to further reduce these errors. Additionally we would like to apply our proposed methods to other multimedia data.

References

1. Falchi, F., Lucchese, C., Orlando, S., Perego, R., Rabitti, F.: A metric cache for similarity search. In: LSDS-IR 2008: Proceeding of the 2008 ACM Workshop on Large-Scale Distributed Systems for Information Retrieval, pp. 43–50. ACM, New York (2008)
2. Zezula, P., Amato, G., Dohnal, V., Batko, M.: Similarity Search: The Metric Space Approach. Springer, Secaucus (2005)
3. Hanan, S.: Foundations of Multidimensional and Metric Data Structures. Morgan Kaufmann Publishers Inc., San Francisco (2005)
4. Hjaltason, G.R., Samet, H.: Index-driven similarity search in metric spaces (survey article). ACM Trans. Database Syst. 28(4), 517–580 (2003)
5. Chavez, E., Navarro, G., Baeza-Yates, R., Marroquin, J.L.: Searching in metric spaces. ACM Comput. Surv. 33(3), 273–321 (2001)
6. Tuncel, E., Ferhatosmanoglu, H., Rose, K.: Vq-index: An index structure for similarity searching in multimedia databases. In: MULTIMEDIA 2002: Proceedings of the tenth ACM International Conference on Multimedia, pp. 543–552. ACM, New York (2002)
7. Weber, R., Schek, H.J., Blott, S.: A quantitative analysis and performance study for similarity-search methods in high-dimensional spaces. In: VLDB 1998, pp. 194–205. Morgan Kaufmann, San Francisco (1998)
8. Urago, Y., Tashima, K., Aoki, T., Iwasaki, Y., Shinohara, T.: Video identification system using high-speed search of approximation images by the spatial indexes. In: IPSJ Kyushu Chapter Symposium (2009) (in Japanese)
9. Zezula, P., Savino, P., Amato, G., Rabitti, F.: Approximate similarity retrieval with m-trees. The VLDB Journal 7(4), 275–293 (1998)
10. Amato, G.: Approximate Similarity Search in Metric Spaces. PhD thesis, University of Dortmund (2002)
11. Kamel, I., Faloutsos, C.: Hilbert r-tree: An improved r-tree using fractals. In: VLDB 1994: Proceedings of the 20th International Conference on Very Large Data Bases, pp. 500–509. Morgan Kaufmann Publishers Inc., San Francisco (1994)
12. Hjaltason, G.R., Samet, H.: Properties of embedding methods for similarity searching in metric spaces. IEEE Trans. Pattern Anal. Mach. Intell. 25(5), 530–549 (2003)
13. Shinohara, T., Ishizaka, H.: On dimension reduction mappings for approximate retrieval of multi-dimensional data. In: Progress in Discovery Science, London, UK, pp. 224–231. Springer, Heidelberg (2002)
14. Navarro, G.: Searching in metric spaces by spatial approximation. The VLDB Journal 11(1), 28–46 (2002)
15. Kalantari, I., McDonald, G.: A data structure and an algorithm for the nearest point problem. IEEE Trans. Softw. Eng. 9(5), 631–634 (1983)
16. Uhlmann, J.K.: Satisfying general proximity/similarity queries with metric trees. Inf. Proc. Letters 40(4), 175–179 (1991)
17. Chávez, E., Navarro, G.: A compact space decomposition for effective metric indexing. Pattern Recogn. Lett. 26(9), 1363–1376 (2005)

Estimating the Influence of Documents in IR Systems: A Marked Indexing Approach*

Ye Wang[1], Yi Han[2], and Tianbo Lu[3]

[1] Central South University, China
[2] National University of Defense Technology, China
[3] Beijing University of Posts and Telecommunications, China

Abstract. In modern information retrieval (IR) systems, scoring functions have been extensively adopted for sorting results. For a given document, the rank in sorted result lists with respect to hot searches can be considered as its influence. When a new document comes, can we use such IR systems to evaluate its influence before we insert it into the corpus? Such issue may not be solved very well by current IR systems with inverted indexes. In this paper, an influence measure based on documents' global rank is proposed, and the inverted index structure has been extended by adding the position milestones for speeding up the ranking calculation. Moreover, a performance study using both real data and synthetic data verifies the effectiveness and the efficiency of our method.

Keywords: Vector Space Model, Scoring function, Inverted Index, Milestones, Influence.

1 Introduction

Since 1990s, with the rapid development of information technology and popularization of Internet applications, a large number of web-based documents have been generated for meeting the increasing demand of people. However, massive data also brought a lot of challenges to organize, storage and retrieve the information. During the last decade, with the increasing number of massive data management systems, the information retrieval(IR) systems also got great development. IR systems provide a flexible and user-friendly way: When a user types a set of terms(keywords) into an IR system, the system examines its index and provides a listing of best-matching documents according the relevance to the query. At the same time, vector space model, an important model for measuring

* The research of Yi Han was supported in part by by China National High-tech R&D Program (863 Program) under Grant No. 2007AA010502 and National Natural Science Foundation of China under Grant No. 60873204 and 60933005. All opinions, findings, conclusions and recommendations in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 263–272, 2010.

the similarity between documents, has also been extensively used for measuring of relevance between queries and answers in such systems.

Vector space model [1] is an algebraic model, which has been applied in information filtering, information retrieval, indexing and relevancy rankings. In this model, both documents and queries are represented as multi-dimensional vectors, and each dimension in them corresponds to a separate term. If a term occurs in a document or a query, the value in corresponding dimension is non-zero. The relevance between documents and queries can be calculated by comparing the deviation of angles between their corresponding vectors.

$$relevance(\mathbf{d}, \mathbf{q}) = \cos\theta = \frac{\mathbf{d} \cdot \mathbf{q}}{\|\mathbf{d}\| \, \|\mathbf{q}\|} \tag{1}$$

Equation 1 illustrates the cosine similarity, which is an example of vector space model. $\cos\theta = 0$ indicates that the document $\mathbf{d}$ and query $\mathbf{q}$ are orthogonal, that is, the document $\mathbf{d}$ does not contain the search terms of $\mathbf{q}$.

Since there might be millions of relevant results to a given query, people may not be patient to go through all the listed documents. Most IR systems employ relevancy functions to rank the results to provide the "best" results first. In other words, the rank of a document with respect to a given query determines the probability of the document being accessed in entire corpus [2]. Therefore, in this paper, we consider the ranks of a given document with respect to different queries as the its influence.

However, for a newly coming document with content to be determined, can we estimate the its influence before inserting it to the current corpus? Analysis on influence of given documents in advance plays an important role and has brilliant prospects on advertising revenue estimation, social impact assessment, and other areas.

Definition 1 (Rank Estimation). *In a corpus C, for a term t and a document $\mathbf{d} = \langle t_1, \ldots, t_m \rangle \in C$, $\mathbf{d}$ ranks with respect to t in the $\mathbf{w}$th place if, and only if there exists $\mathbf{w} - \mathbf{1}$ other documents $\mathbf{d}' \in C$ such that $relevance(\mathbf{d}', t) > relevance(\mathbf{d}, t)$. The rank of $\mathbf{d}$ with respect to t is denoted by $Rank(\mathbf{d}, t)$. For a given ϵ, an estimated rank of $\mathbf{d}$ with respect to t, denoted by $Rank_\epsilon(\mathbf{d}, t)$, returns a value such that*

$$|Rank_\epsilon(\mathbf{d}, t) - Rank(\mathbf{d}, t)| \leq \epsilon.$$

$Rank_\epsilon(\mathbf{d}, k)$ returns an estimated rank of a given document with respect to a selected keyword. For real applications, people only need the approximate page number of the given document located in but not the exact ranking position, we introduce ϵ as a parameter for controlling the error bound. For estimating the page number $\mathbf{d}$ located in, ϵ should be equivalent to the number of items in a single result page.

Please note that the rank is a global concept, that is, if we want to calculate the rank of d with respect to k, a naïve way is we firstly calculate the values of scoring

function of all the other documents and compare them with $relevance(d, k)$. In such way, at least $|C| - \epsilon$ calculations of relevance and $|C| - 1 - \epsilon$ comparisons are needed($|C|$ is the number of document in corpus C). For a document d with large number of terms, and a corpus with large number of documents, suppose a comprehensive influence analysis on d needs to calculate the ranks with respect to all the possible keywords, in proposed naïve way, relevance value for each document with respect to each terms in d has to be calculated. The the running cost of such naïve solution will be extremely large and unaffordable.

In IR systems, for speeding up the calculation and eliminate the irrelevant candidates, inverted indexes have been widely used. For evaluating the influence of a given document, we can insert it into the corpus, update the index, and execute the query to get the document's ranking. By using inverted indexes, the relevance calculations and comparisons can be limited in the set of documents containing k. However, for some popular keywords the number of relevance documents is still a very large number. Moreover, such procedures will update the index frequently. Especially for these documents whose content is to be determined, repeated and frequent updates on indexes will bring a large number of fragments, and the overall efficiency will also be affected. How to estimate the rank of newly coming documents with respect to particular queries without bringing to much performance loss is still a practical and challenge problem.

In this paper, for estimating the influence of documents in a given corpus, we propose an efficient index structure by adding a set of milestones. Moreover, we also designed a high-speed, scalable index update strategy for it. The rest of the paper is organized as follows. Section 2 reviews the basic principles of inverted index. Section 3 discusses the system architecture, algorithms and update strategy. A systematic empirical study conducted on the multiple data sets is reported in Section 4. Section 5 concludes the paper.

2 Related Work

Our work is highly related to the previous studies on document influence analysis, indexing and scoring. In this section, we review some representative work briefly.

2.1 Ranking Functions

Documents influence analysis has been conducted in many aspects. Some previous studies focused on analyzing static properties of documents. The TFIDF [7] (en.wikipedia.org/TFIDF) measure (term frequencyCinverse document frequency) is the one of most famous scoring functions, and it is often used in IR systems and text mining. This weight is a statistical measure used to evaluate how important a word is to a document in a collection or corpus. The importance increases proportionally to the number of times a word appears in the document but is offset by the frequency of the word in the corpus. Variations of the TFIDF weighting scheme are often used by search engines as a central tool in scoring and ranking a document's relevance given a user query.

Several well known link-based ranking algorithms such as PageRank [3] and HITS [4] have been introduced for ranking pages on the web. For each document, the amount of influence is decided by the number of citations and the influence of referrers. Such methods can be applied to measure the importance of documents in citation network. However, since those link-based methods are mainly designed for networks, they are content independent, and can not be applied to estimate the rank either.

2.2 Inverted Indexes

The inverted index [5,6,7] is the most popular data structure used in document retrieval systems. There are some variants of inverted indexes for different propose. In this paper, the inverted index is just for fast retrieving the documents containing selected terms.

In this paper, an inverted index stores a mapping $\langle t, ref \rangle$ from terms to a list of references to documents containing corresponding terms. For speeding up the searching process, we suppose all the items(documents) in reference list are sorted with in corresponding relevance descending order. When a search query (keyword) comes, IR system returns the reference list directly.

3 Indexing Approaches

For a document d, and a corpus C, suppose a comprehensive influence analysis on d needs to calculate $Rank_\epsilon(d, k)$ with respect to all the possible terms $t \in d$, we propose a straightforward solution based on inverted indexes.

3.1 A Straightforward Approach

We build an inverted index for entire corpus, and sort all the reference list in relevance descending order. To calculate the ranks $Rank(d, k)$ with respect to all the possible terms $t \in d$, we scan the corresponding sorted reference list, until d is found. Algorithm 1 gives the pseudocode.

To calculate the rank for a given document d with respect of all the possible terms $\{t|t \in d\}$, the straightforward method has to do $\sum_{t:t\in d} |\{d_j|t \in d_j\}|$ calculations of relevance.

For a corpus with large number of documents and terms, it's impossible for storing all the relevance values in the system. Therefore, for locating d in t's reference list, we employ the binary insertion method [8,9] to eliminate the unnecessary comparisons and re-calculations of relevance.

3.2 Extended Indexes with Milestones

Since it's impossible for storing all the relevance values in the system, we design an extended inverted index for fast locating a given document. Figure 1 shows

Algorithm 1. A straightforward algorithm

Input: a given document d_n, corpus C;
Output: influence vector $R = r_1, \ldots, r_m$;
Initialization:
build the inverted index
for each term t **do**
  for each document d in t's reference list **do**
    calculate $relevance(d, t)$;
  end for
  sort $t.ref$ in relevance descending order;
end for
Calculation:
let $i = 0$; //ith term in d_n
for each term $t \in d_n$ **do**
  let $left = 0$,$right = |\{d|t \in d\}|$; //reference's length
  calculate $relevance(d, t)$;
  while $left < right$ **do**
    let $middle = (left - right)/2$;
    calculate $relevance(t.ref_{middle}, t)$;
    if $relevance(d, t) \leq relevance(t.ref_{middle}, t)$ **then**
      let $left = middle + 1$;
    else
      let $right = middle$;
    end if
  end while
  let $r_i = right$, $i = i + 1$;
end for
output r;

the system architecture. The extension of the index structure has self-updating and self-adjustment capability. When new documents come, the index updates automatically, and transparently conduct self-adjustment and optimization.

When a user enters a keyword search query, the system returns the reference list by pages; when the user issues an influence estimation query, the system only fetches a small part of reference lists from the inverted index, and makes the comparisons with them. The results will be returned to user by index plugin directly.

Figure 2 shows an example of extended inverted indexes. For fast estimate the rank for given documents, we add following features:

- Sort all the reference list in document relevance descending order.
- For 0th, kth, $2k$th, ..., nkth positions of each reference list, the mapping of $\langle relevance, rank \rangle$ will be recorded.

In this paper, we call such position tags as milestones. In our implementation, the milestones will be stored separately as a form of plugin, so it's unnecessary

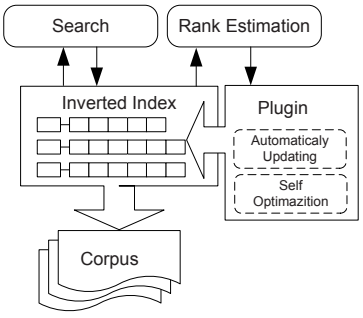


Fig. 1. The system architecture

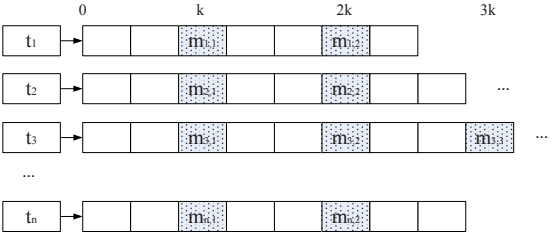


Fig. 2. Extended Inverted Index, k=3

to modify the original inverted index. When a new influence estimation query d comes, for each term $t \in d$, the system only calculates $relevance(d, t)$ and compare it with the milestones, then d will be roughly located with the error bound of k. If we make k equivalent with number of items in result page, the page number will be calculated easily with above procedures. Algorithm 2 gives the pseudocode.

With extended index, for an influence estimate query, there are only $\sum_{t_i:t_i \in d} \log(\frac{|\{d_j|t_i \in d_j\}|}{k})$ comparisons made, and no re-calculations of relevance needed.

3.3 Update the Index

When corpus evolves, the extended index should be updated. For any insertion or deletion of document d, there are $|\{d|t \in d\}|$ reference lists will be updated. For a fast changing corpus, how to avoid performance loss and index fragment caused by frequent index updates is still a challenge problem. We propose update strategy with fully considering the trade-off between performance of query processing and index updating:

Algorithm 2. The algorithm with extended inverted index

Input: a given document d_n, corpus C;
Output: influence vector $R = r_1, \ldots, r_m$;
Initialization:
build the inverted index
for each term t **do**
  for each document d in t's reference list **do**
    calculate $relevance(d, t)$;
  end for
  sort $t.ref$ in relevance descending order;
  for $i = 0 : \frac{|\{d|t \in d\}|}{k}$ **do**
    save $milestones(t, i)$;
  end for
end for
Calculation:
let $i = 0$; //ith term in d_n
for each term $t \in d_n$ **do**
  let $left = 0, right = \frac{|\{d|t \in d\}|}{k}$; //reference's length
  calculate $relevance(d, t)$;
  while $left < right$ **do**
    let $middle = (left - right)/2$;
    if $relevance(d, t) \leq milestones(t, middle)$ **then**
      let $left = middle + 1$;
    else
      let $right = middle$;
    end if
  end while
  let $r_i = right$, $i = i + 1$;
end for
output r;

Only $k-1 : 2(k-1)$ positions will be kept between the milestones. If a new document comes, and the proper area already exists $2k-1$ continuous positions without any milestones among them, this area will be split evenly by a new milestone.

Figure 3 illustrates the update process. There already exists 4 continues positions and d should be inserted among them, so a new milestone $m_{n,i'}$ is set for splitting this area.

4 Environmental Results

We designed an information management system based on the Apache Software Foundation's unstructured information management architecture (UIMA) platform, and conduct the experiments on it. Table 1 describes its detailed configuration. we implement the algorithms with the Java language, and run the programs on CentOS, an operating system with Linux-based kernel.

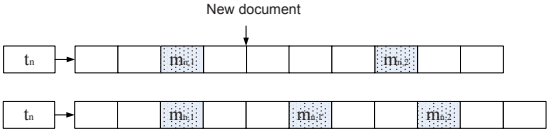


Fig. 3. Update the index, k=3

Table 1. Configuration

IDE	Java SDK 1.6 + Eclipse3.0	
Hardware	CPU	Intel Core Quad 2.83GHz
	Memory	8GB
Software	OS	CentOS kernel ver 2.6.18
	JRE	Java Runtime Environment 1.6
	AS	Apache UIMA

For testing the effectiveness of our method, we carefully selected 3 different kinds of text data sets. SMS09 is a synthetic data set based on randomly reorganized short messages retrieved from the Web; News09 is the news web pages that we collect from Chinese news web sites; Enron [10] is a released e-mail data set (`http://www-2.cs.cmu.edu/~enron`). Table 2 shows the statistics. Since the particular grammatical structure of Chinese text, we employed the segmentation tools developed by Institute of Computing Technology, Chinese Academy of Sciences (`http://ictclas.org/Down_OpenSrc.asp`) for News09 and SMS09. Moreover, a word stoplist is also adopted for eliminating the useless words.

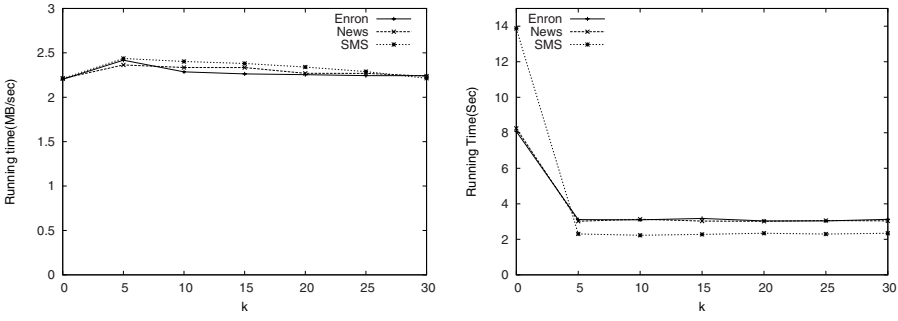
In the experimental section, we use weighted TFIDF [7], an instance of Vector Space Model, as the relevance measuring function. We tested the running time of our algorithm with respect to variable k values. Considering there are large differences in data scale, we used megabytes/second (MB/s) as the standard unit. For the Chinese data sets, running time of word segmentation in not included.

For establishing the indexes, please note that there is no obvious discrimination on running time with respect to different values of k. Building the original inverted index still dominates the running time.

For testing the efficiency of executing the queries, we randomly generate query document with size of 200 words, and we use 1K generated documents as a timing unit for testing the processing time. Figure 4b shows the result. Please note that, by setting the milestones, the executing efficiency has been significantly

Table 2. Statistics of data sets

Name	Type	Language	Scale	Average # of words
SMS09	synthetic	Chinese	4,127,427 documents	32 words
Enron	real	English	517,431	286 words
News09	real	Chinese	5,700	731 words



(a) building index (b) executing queries

Fig. 4. Running time, k=0 means no milestone on the index

improved. For SMS data sets, since it contains much more documents, we infer that the average length of reference lists is larger than the others. Therefore, by setting the milestones, the executing time got more improvements on it.

5 Conclusion

Analyzing the documents' influence has brilliant prospects on advertising revenue estimation, social impact assessment, and other areas. In this paper, we proposed a novel method to measure and calculate the documents' global influence, and the experimental results conducted on both synthetic and real data sets indicate that our supportiveness measures are meaningful, and our methods are efficient in practice.

There are some interesting future directions. For example, we only considered queries with single keyword. In IR systems, multiple-keywords or semantic queries are also very important and should be taken in to account. The proposed influence measure can be combined with malicious ranking, spam detection and so on to carry out further research.

References

1. Salton, G., Wong, A., Yang, C.S.: A vector space model for automatic indexing. Commun. ACM 18(11), 613–620 (1975)
2. Brin, S., Page, L.: The anatomy of a large-scale hypertextual web search engine. Computer Networks 30(1-7), 107–117 (1998)
3. Page, L., Brin, S., Motwani, R., Winograd, T.: The pagerank citation ranking: Bringing order to the web. Technical report, Stanford University (1998)
4. Kleinberg, J.M.: Authoritative sources in a hyperlinked environment. In: Proceedings of the 9th Annual ACM-SIAM Symposium on Discrete Algorithm (SODA 1998), pp. 668–677. ACM Press, New York (1998)

5. Salton, G., McGill, M.: Introduction to Modern Information Retrieval. McGraw-Hill Book Company, New York (1984)
6. Baeza-Yates, R.A., Ribeiro-Neto, B.A.: Modern Information Retrieval. ACM Press / Addison-Wesley (1999)
7. Salton, G., Buckley, C.: Term-weighting approaches in automatic text retrieval. Inf. Process. Manage. 24(5), 513–523 (1988)
8. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms, 2nd edn. The MIT Press and McGraw-Hill Book Company (2001)
9. Knuth, D.E.: The Art of Computer Programming. Sorting and Searching, vol. III. Addison-Wesley, Reading (1973)
10. Klimt, B., Yang, Y.: The enron corpus: A new dataset for email classification research. In: ECML, pp. 217–226 (2004)

String Matching with Mismatches by Real-Valued FFT

Kensuke Baba

Research and Development Division, Kyushu University Library
10-1, Hakozaki 6, Higashi-ku, Fukuoka, 812-8581, Japan
baba@lib.kyushu-u.ac.jp

Abstract. String matching with mismatches is a basic concept of information retrieval with some kinds of approximation. This paper proposes an FFT-based algorithm for the problem of string matching with mismatches, which computes an estimate with accuracy. The algorithm consists of FFT computations for binary vectors which can be computed faster than the computation for vectors of complex numbers. Therefore, a reduction of the computation time is obtained by the speed-up for FFT, which leads an improvement of the variance of the estimates. This paper analyzes the variance of the estimates in the algorithm and compares it with the variances in existing algorithms.

Keywords: String matching with mismatches, FFT, randomized algorithm.

1 Introduction

Similarity on strings is one of the most important concepts in applications of information retrieval which cannot be explained completely by modeling in terms of sequences and the exact matching on it, such as, mining on a huge data base and homology search in biology. The problem of *string matching* is to find the occurrences of a (short) string called a *pattern* in a (long) string called a *text*. The problem of *string matching with mismatches* is to compute the vector whose element is the number of the matches between the pattern and every substring of the text whose length is equal to the pattern. Namely, the vector for the problem of string matching with mismatches solves generally the problem of string matching which allows substitutions of a character to introduce the variations of a pattern. It is useful for many applications of information retrieval to develop an efficient algorithm for the problem of string matching with mismatches.

For the problem of string matching with mismatches with a pattern of length m and a text of length n, there exists an $O(n \log m)$ algorithm which is based on the fast Fourier transformation (FFT), while the naive comparison-based algorithm takes $O(mn)$ time. This approach was essentially developed by Fischer and Paterson [6]. In this algorithm, two strings are converted into binary strings with respect to each character in the alphabet for the numerical computation of FFT. Hence, the computation of the algorithm is the σ-times iteration of

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 273–283, 2010.

the $O(n \log m)$ computation of FFT for the alphabet size σ. Atallah *et al.* [1] introduced a randomized algorithm to reduce the iteration number by a trade-off with the accuracy of the estimates for the vector. In the algorithm, a text and a pattern are converted into two sequences of complex numbers by a function chosen randomly from the set of size σ^σ.

The aim of this paper is to improve the accuracy of the estimates in the randomized algorithm for string matching with mismatches. Schoenmeyr and Yu-Zhang [10] modified the previous algorithm such that the functions which convert characters into complex numbers are restricted to the bijective functions, and therefore the size of the set is $\sigma!$. The upper bound of the variance of the estimates decreases and it is notable for small alphabets. Nakatoh *et al.* [8,9] reduced the size of the set of functions which covert characters into complex numbers to $2\sigma - 2$ [8] and $\sigma - 1$ [9]. Since the sizes of the sets are small compared with those in the previous two algorithms, the variance decreases greatly in the case where the sampling of the function is operated without replacement.

The main idea of our method is an improvement of the variance of the estimates by reducing the computation time of the $O(n \log m)$ computation of FFT. By converting strings to vectors of binary numbers instead of complex numbers, the practical computation time of a single operation of FFT can be reduced [11]. Therefore, the iteration number in a given time, that is, the number of the samples for an estimate increases, which implies an improvement of the variance since the variance is inverse proportion to the number of samples. Baba *et al.* [2] proposed a randomized algorithm as an improvement of the algorithm in [1]. In this algorithm, each character is converted into 1 or -1 and the number of the possible functions from Σ to $\{-1, 1\}$ is 2^σ. In this paper, we propose an algorithm in which

- input strings are converted to vectors on $\{-1, 1\}$,
- the upper bound of the variance of the estimates is explicitly lower than that in the algorithm in [2],
- the size of the population for samples is $\sigma - 1$ if σ is a power of two.

Therefore, the accuracy of the estimates of the proposing algorithm is better than [2], and expected to be better than the other existing algorithms if some fast algorithms are applied to the computation of FFT for binary vectors.

2 Preliminaries

Let $\mathbf{N}$ be the set of non-negative integers. Let Σ be an alphabet and Σ^n the set of the strings of length $n \in \mathbf{N}$ over Σ. The size of a set S is denoted by $|S|$. The j-th character of a string $s \in \Sigma^n$ is denoted by s_j for $1 \leq j \leq n$. The j-th element of an n-dimensional vector v is denoted by v_j for $1 \leq j \leq n$.

Let δ be the Kronecker function from $\Sigma \times \Sigma$ to $\{0, 1\}$, that is, for $a, b \in \Sigma$, $\delta(a, b)$ is 1 if $a = b$, and 0 otherwise. Then, for $t \in \Sigma^n$ and $p \in \Sigma^m$, the j-th element of the *score vector* $C(t, p)$ between t and p is

$$c_j = \sum_{k=1}^{m} \delta(t_{j+k-1}, p_k)$$

for $1 \leq j \leq n - m + 1$. The problem of *string matching with mismatches* is to compute the score vector for two strings.

Example 1. The score vector between $t = \texttt{adcbabac}$ and $p = \texttt{abac}$ is $C(t, p) = (1, 0, 2, 0, 4)$.

The discrete Fourier transformation (DFT) of an n-dimensional vector v is the n-dimensional vector V of which k-th element is

$$V_k = \sum_{j=1}^{n} v_j \cdot \omega_n^{(j-1)(k-1)}$$

for $1 \leq k \leq n$, where $\omega_n = e^{2\pi i/n}$ and $i^2 = -1$. Let u and v be n-dimensional vectors and w the correlation of u and v, that is, for $1 \leq k \leq n$

$$w_k = \sum_{j=1}^{n} u_j \cdot v_{j+k},$$

where $v_{n+j} = v_j$ for $1 \leq j \leq n - 1$. Let U, V, and W be the DFTs of u, v, and w, respectively. Then, by the basic property of DFT, for $1 \leq j \leq n$

$$W_j = U_j \cdot \overline{V_j},$$

where $\overline{c}$ is the conjugate complex number of c. The DFT and its inverse (IDFT) of an n-dimensional vector can be computed in $O(n \log n)$ time by FFT, respectively. Therefore, w is computed from u and v in $O(n \log n)+O(n)+O(n \log n) = O(n \log n)$ time [4].

Lemma 1. *The correlation of two n-dimensional vectors can be computed in $O(n \log n)$ time.*

3 Deterministic Algorithm

Let H_n be an n-dimensional Hadamard's matrix for $n \in \mathbf{N}$, that is, any element of H_n is -1 or 1 and

$$H_n^T H_n = nI_n,$$

where M^T is the transposed matrix of a matrix M and I_n is the n-dimensional unit matrix. It is known that H_n exists if n is a power of two.

Example 2.

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Let $\sigma = |\Sigma|$ and $\Sigma = \{a_1, a_2, \ldots, a_\sigma\}$. $M(j,k)$ denotes the (j,k)-element of a matrix M. We assume that H_σ exists for σ. For $1 \leq \ell \leq \sigma$, ϕ_ℓ is defined to be the function from Σ to $\{-1, 1\}$ such that

$$\phi_\ell(a_j) = H_\sigma(j, \ell)$$

for $1 \leq j \leq \sigma$. Then, by the property of Hadamard's matrix,

$$\sum_{\ell=1}^{\sigma} \phi_\ell(a_j) \cdot \phi_\ell(a_k) = \sum_{\ell=1}^{\sigma} H_\sigma(j, \ell) \cdot H_\sigma(k, \ell) = \sigma\delta(a_j, a_k)$$

for any $1 \leq j, k \leq \sigma$. Therefore, the score vector between $t \in \Sigma^n$ and $p \in \Sigma^m$ is

$$\begin{aligned} c_j &= \sum_{k=1}^{m} \delta(t_{j+k-1}, p_k) \\ &= \sum_{k=1}^{m} \left(\frac{1}{\sigma} \sum_{\ell=1}^{\sigma} \phi_\ell(t_{j+k-1}) \cdot \phi_\ell(p_k) \right) \\ &= \frac{1}{\sigma} \sum_{\ell=1}^{\sigma} \sum_{k=1}^{m} \phi_\ell(t_{j+k-1}) \cdot \phi_\ell(p_k) \quad (1 \leq j \leq n - m + 1). \end{aligned}$$

Let s^ℓ be the $(n - m + 1)$-dimensional vector such that

$$s^\ell_j = \sum_{k=1}^{m} \phi_\ell(t_{j+k-1}) \cdot \phi_\ell(p_k) \quad (1 \leq j \leq n - m + 1) \tag{1}$$

for $1 \leq \ell \leq \sigma$. Let τ be the n-dimensional vector $(\phi_\ell(t_j))$, and π the m-dimensional vector $(\phi_\ell(p_j))$ for each ℓ. Then, s^ℓ is a part of the correlation of τ and π' which is obtained by padding $n - m$ 0's to π. Therefore, by Lemma 1, s^ℓ is computed from τ and π' in $O(n \log n)$ time.

Additionally, the following standard technique [5] is applied. We part τ into overlapping chunks each of size $(1+\alpha)m$. One chunk and the $(1+\alpha)m$-dimensional vector π' with α 0's yield $\alpha m + 1$ elements of s^ℓ. Since we have $n/\alpha m$ chunks and each chunk can be computed in $O((1 + \alpha)m \log((1 + \alpha)m))$ time, the total time complexity is $(n/\alpha m) \cdot O((1+\alpha)m \log((1+\alpha)m)) = O(n \log m)$ by choosing $\alpha = O(m)$.

Thus, since a single correlation is computed for a single ϕ_ℓ and $1 \leq \ell \leq \sigma$, the score vector $C(t, p)$ is obtained by repeating the $O(n \log m)$ computation σ times. Even if we consider the assumption of the existence of the Hadamard's matrix, the iteration number is less than 2σ. The algorithm is summarized in Figure 1.

Theorem 1. *The deterministic algorithm A computes the score vector between $t \in \Sigma^n$ and $p \in \Sigma^m$ in $O(\sigma n \log m)$ time.*

In the rest of this section, we analyze the number of the $O(n \log m)$ computations in the iteration in terms of σ in the strict sense.

A:
Input: a text $t \in \Sigma^n$ and a pattern $p \in \Sigma^m$
Output: the score vector $C(t,p) = (c_1, c_2, \ldots, c_{n-m+1})$

Let H_ν be a ν-dimensional Hadamard's matrix for $\nu \geq \sigma = |\Sigma|$ and $\phi_\ell(a_j) = H_\nu(j,\ell)$ for $1 \leq \ell \leq \nu$ and $a_j \in \Sigma$.

1. For $1 \leq \ell \leq \nu$,
1.1. compute $T_i^\ell = \phi_\ell(t_i)$ for $1 \leq i \leq n$ and $P_i^\ell = \phi_\ell(p_i)$ for $1 \leq i \leq m$,
1.2. compute $s_j^\ell = \sum_{k=1}^{m} T_{j+k-1}^\ell \cdot P_k^\ell$ for $1 \leq j \leq n-m+1$ by FFT;
2. compute $c_i = \frac{1}{\nu} \sum_{\ell=1}^{\nu} s_j^\ell$ for $1 \leq j \leq n-m+1$.

Fig. 1. The deterministic algorithm A for the problem of string matching with mismatches

By the argument of the existence of the Hadamard's matrix, the iteration number is at least σ and at most $2\sigma - 2$. Moreover, if we construct H_σ by Sylvester's method, that is, $H_1 = [1]$ and for $1 \leq k \leq \log \sigma$

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}$$

is applied recursively, then $\phi_1(a_j) = 1$ for any $1 \leq j \leq \sigma$. Therefore, we can skip a single $O(n \log m)$ computation for $\ell = 1$. Thus, the iteration number μ is

$$\sigma - 1 \leq \mu \leq 2\sigma - 3.$$

4 Randomized Algorithm

We assume that σ is a power of two. A *sample* of the score vector is the $(n-m+1)$-dimensional vector s^ℓ in Equation 1. An *estimate* of the score vector is defined to be

$$\hat{s_j} = \frac{1}{h} \sum_{\ell \in L} s_j^\ell \quad (1 \leq j \leq n-m+1), \tag{2}$$

where L is a set of h integers which are chosen independently and uniformly from $\{1, 2, \ldots, \sigma\}$. The algorithm is described in Figure 2.

The expectation of x is described by $E[x]$ and the variance by $V[x]$. For $1 \leq j \leq n-m+1$,

$$E[\hat{s_j}] = c_j$$

since $E\left[s_j^\ell\right] = c_j$. By the definition of ϕ_ℓ, $|\phi_\ell(a_j) \cdot \phi_\ell(a_k)| = 1$ and $(\phi_\ell(a_j))^2 = 1$ for any $1 \leq j, k, \ell \leq \sigma$, and hence $-(m - c_j) \leq s_j^\ell - E[s_j^\ell] \leq m - c_j$ for any $1 \leq \ell \leq \sigma$ and $1 \leq j \leq n-m+1$. Therefore,

B:
Input: a text $t \in \Sigma^n$, a pattern $p \in \Sigma^m$, and the number h of the samples
Output: an estimate $(\hat{s_1}, \hat{s_2}, \ldots, \hat{s_{n-m+1}})$ of the score vector $C(t,p)$

Let H_ν be a ν-dimensional Hadamard's matrix for $\nu \geq \sigma = |\Sigma|$ and
$\phi_\ell(a_j) = H_\nu(j,\ell)$ for $1 \leq \ell \leq \nu$ and $a_j \in \Sigma$.

1. Make a set L of h integers randomly chosen from $\{1, 2, \ldots, \nu\}$;
2. For $\ell \in L$,
2.1. compute $T_i^\ell = \phi_\ell(t_i)$ for $1 \leq i \leq n$ and $P_i^\ell = \phi_\ell(p_i)$ for $1 \leq i \leq m$,
2.2. compute $s_j^\ell = \sum_{k=1}^{m} T_{j+k-1}^\ell \cdot P_k^\ell$ for $1 \leq j \leq n-m+1$ by FFT;
3. compute $\hat{s_i} = \frac{1}{h} \sum_{\ell \in L} s_j^\ell$ for $1 \leq j \leq n-m+1$.

Fig. 2. The randomized algorithm B for the problem of string matching with mismatches

$$\begin{aligned} V[\hat{s_j}] &= \frac{1}{h} V\left[s_j^\ell\right] \\ &= \frac{1}{h}\left(\frac{1}{\sigma}\sum_{\ell=1}^{\sigma}\left(s_j^\ell - E[s_j^\ell]\right)^2\right) \\ &\leq \frac{(m-c_j)^2}{h}. \end{aligned}$$

This upper-bound of the variance does not depend on σ, and therefore the same result is obtained for any Σ by considering H_ν for a power of two $\nu \geq \sigma$ instead of H_σ.

Theorem 2. *The randomized algorithm B computes an estimate for the score vector between $t \in \Sigma^n$ and $p \in \Sigma^m$ in $O(hn \log m)$ time for the number h of samples. The expectation of the estimates is equal to c_j and the variance of the estimates is bounded by $(m-c_j)^2/h$ for $1 \leq j \leq n-m+1$.*

In the case where the Hadamard's matrix is Sylvester-type, the variance of the estimates of the score vector decreases.

Let ν be the power of two such that $\sigma \leq \nu < 2\sigma$. Then,

$$\sum_{\ell=2}^{\nu} \phi_\ell(a_j) \cdot \phi_\ell(a_k) = \sum_{\ell=1}^{\nu} H_\nu(j,\ell) \cdot H_\nu(k,\ell) - 1 = \nu\delta(a_j, a_k) - 1$$

and hence the score vector is

$$\begin{aligned} c_j &= \sum_{k=1}^{m}\left(\frac{1}{\nu}\sum_{\ell=2}^{\nu}\phi_\ell(t_{j+k-1}) \cdot \phi_\ell(p_k) + \frac{1}{\nu}\right) \\ &= \frac{1}{\nu-1}\sum_{\ell=2}^{\nu}\left(\frac{\nu-1}{\nu}\sum_{k=1}^{m}\phi_\ell(t_{j+k-1}) \cdot \phi_\ell(p_k) + \frac{m}{\nu}\right) \quad (1 \leq j \leq n-m+1). \end{aligned}$$

An estimate $(\hat{s_j})$ of the score vector is defined by Equation 2 for the following sample

$$s_j^\ell = \frac{\nu-1}{\nu}\sum_{k=1}^{m}\phi_\ell(t_{j+k-1})\cdot\phi_\ell(p_k) + \frac{m}{\nu} \quad (1 \le j \le n-m+1)$$

for $2 \le \ell \le \nu$.

For $1 \le j \le n-m+1$, clearly $E[\hat{s_j}] = c_j$ and, by the basic properties of variance,

$$\begin{aligned} V[\hat{s_j}] &= \frac{1}{h}V\left[s_j^\ell\right] \\ &= \frac{(\nu-1)^2}{\nu^2 h}V\left[\sum_{j=1}^{m}\phi_\ell(t_{j+k-1})\cdot\phi_\ell(p_j)\right] \\ &\le \frac{(\nu-1)^2}{\nu^2 h}\left(\sum_{j=1}^{m}\sqrt{V\left[\phi_\ell(t_{j+k-1})\cdot\phi_\ell(p_j)\right]}\right)^2. \end{aligned}$$

By the definition of ϕ_ℓ, $V\left[\phi_\ell(a)\cdot\phi_\ell(a)\right] = 0$ for any $a \in \Sigma$. In the case where $a \ne b$, since $\left(\phi_\ell(a)\cdot\phi_\ell(b)\right)^2 = 1$,

$$\begin{aligned} V\left[\phi_\ell(a)\cdot\phi_\ell(b)\right] &= E\left[\left(\phi_\ell(a)\cdot\phi_\ell(b)\right)^2\right] - E\left[\phi_\ell(a)\cdot\phi_\ell(b)\right]^2 \\ &= \frac{1}{\nu-1}\sum_{\ell=2}^{\nu}1 - \left(-\frac{1}{\nu-1}\right)^2 \\ &= \frac{\nu(\nu-2)}{(\nu-1)^2} \end{aligned}$$

for any $a, b \in \Sigma$. Therefore, since $\nu \le 2\sigma - 2$, the variance of the estimates is bounded by

$$\begin{aligned} V[\hat{s_j}] &\le \frac{(\nu-1)^2}{\nu^2 h}\left((m-c_j)\cdot\sqrt{\frac{\nu(\nu-2)}{(\nu-1)^2}} + c_j\cdot 0\right)^2 \\ &= \frac{(\nu-2)(m-c_j)^2}{\nu h} \\ &\le \frac{(\sigma-2)(m-c_j)^2}{(\sigma-1)h} \end{aligned}$$

for $1 \le j \le n-m+1$.

Theorem 3. *In the randomized algorithm B with a Sylvester-type Hadamard's matrix, the variance of the estimates of the score vector is bounded by* $(\sigma-2)(m-c_j)^2/(\sigma-1)h$ *for* $1 \le j \le n-m+1$.

Additionally, in the case where the sampling of ℓ is operated without replacement, by the basic property of the variance,

$$V[\hat{s_j}] \leq \frac{\nu - h - 1}{\nu - 2} \cdot \frac{(\sigma - 2)(m - c_j)^2}{(\sigma - 1)h} = \frac{(2\sigma - h - 3)(m - c_j)^2}{2(\sigma - 1)h}$$

for $1 \leq j \leq n - m + 1$.

5 Related Work

5.1 The Standard Algorithm

The main idea of FFT-based algorithms, which computes the score vector as a correlation (or a convolution) of two numerical vectors in $O(n \log m)$ time for strings of lengths m and n, was essentially developed by Fischer and Paterson [6]. A generalized algorithm on this idea is described simply in [7].

In the standard algorithm, two strings are converted into binary strings with respect to each character in the alphabet for the numerical computation of FFT, and the score vector is the sum of all results of the correlations. Namely, for the functions $\phi_x : \Sigma \to \{0, 1\}$ for $x \in \Sigma$ such that

$$\phi_x(a) = \delta(x, a)$$

for any $a \in \Sigma$, it is clear that

$$\sum_{x \in \Sigma} \phi_x(a) \cdot \phi_x(b) = \delta(a, b)$$

for any $a, b \in \Sigma$. Therefore, the score vector between $t \in \Sigma^n$ and $p \in \Sigma^m$ is

$$c_j = \sum_{x \in \Sigma} \sum_{k=1}^{m} \phi_x(t_{j+k-1}) \cdot \phi_x(p_k) \quad (1 \leq j \leq n - m + 1).$$

Since $\sum_{k=1}^{m} \phi_x(t_{j+k-1}) \cdot \phi_x(p_k)$ for $1 \leq j \leq n - m + 1$ with respect to an $x \in \Sigma$ is computed as a part of a correlation of two vectors, an $O(\sigma n \log m)$ algorithm is obtained in the same way as the algorithm A in Section 3.

5.2 Randomized Algorithms

The computation time of the standard algorithm is not practical for strings over a large alphabet. As a solution of this problem, Atallah *et al.* [1] introduced a Monte Carlo-type algorithm in which the computation time is reduced by a trade-off with the accuracy of the estimates for the score vector. In this algorithm, an estimate is the arithmetic mean of some samples, and a sample is computed with respect to a function which is chosen independently and uniformly from the set of functions from Σ to the set of complex numbers.

Let Φ be the set of the functions from Σ to $\{0, 1, \ldots, \sigma - 1\}$ and $\omega_\sigma = e^{2\pi i/\sigma}$. Then, since $\sum_{j=0}^{\sigma-1} \omega_\sigma^j = 0$,

$$\frac{1}{|\Phi|} \sum_{\phi \in \Phi} \omega_\sigma^{\phi(a)} \cdot \overline{\omega_\sigma^{\phi(b)}} = \frac{1}{|\Phi|} \sum_{\phi \in \Phi} \omega_\sigma^{\phi(a)-\phi(b)} = \delta(a, b)$$

for any $a, b \in \Sigma$. Therefore, the score vector between $t \in \Sigma^n$ and $p \in \Sigma^m$ is

$$c_j = \frac{1}{|\Phi|} \sum_{\phi \in \Phi} \sum_{k=1}^{m} \omega_\sigma^{\phi(t_{j+k-1})} \cdot \overline{\omega_\sigma^{\phi(p_k)}} \quad (1 \le j \le n - m + 1).$$

Thus, a randomized algorithm is obtained in the same way as the algorithm B in Section 4. The expectation of the estimate is equal to the score vector and the variance of the estimates is bounded by $(m - c_j)^2/h$ for the number h of samples. (Strictly, if we regard the real part of the output as the estimate, then the upper bound is $(m - c_j)^2/2h$ [10].)

Schoenmeyr and Yu-Zhang [10] modified the previous algorithm such that Φ is restricted to the set of the bijective functions, and therefore the size of the set is $\sigma!$. The authors claim that the upper bound of the variance of the estimates in their algorithm is $\sigma(\sigma - 3)(m - c_i)^2/2(\sigma - 1)^2 h$, that is, the variance of the estimates decreases and it is notable for small alphabets.

Nakatoh *et al.* [8,9] reduced the size of the set of functions which covert characters into complex numbers to $2\sigma - 2$ [8] and $\sigma - 1$ [9]. The upper bounds of the variance in the previous two algorithms are lower than that in [1]. Moreover, since the sizes of the sets are small compared with those in the previous two algorithms, σ^σ and $\sigma!$, the algorithms by Nakatoh *et al.* can be utilized as deterministic algorithms in the case where σ is small, and the variance decreases greatly in the case where the sampling of the function is operated without replacement.

5.3 Algorithms by Binary Vectors

In the randomized algorithms in the previous subsection, the $O(n \log m)$ computation consists of two DFTs and a single IDFT, and the DFTs are for vectors of complex numbers which are converted from input strings. If the vectors are expressed by vectors of binary numbers such as vectors over $\{0, 1\}$ or $\{-1, 1\}$, some speed-up methods can be applied to the $O(n \log m)$ computation of FFT. Generally, as to FFT for vectors of real numbers, there exist efficient algorithms [11].

First of all, the size of each vector is practically half since a complex number is treated as $a + ib$ for real numbers a and b. Therefore, the computation time is half in some standard FFT algorithms which treat a vector of complex numbers as two vectors of real numbers. Next, the product of a complex number $a + ib$ and a real number d can be computed in a short time compared with the product of $a + ib$ and a complex number $a' + ib'$, that is, the numbers of products of real numbers are 2 and 4, respectively. (Note that even if we consider vectors of real numbers, it remains computations with complex numbers in FFT.) Additionally, in the case

where d is 1, -1, or 0, the products in the computations of DFTs can be ignored, and hence the number of products decreases greatly in a practical sense.

The standard algorithm, in which input strings are converted into binary vectors, can be randomized in the same way as the algorithms in the previous subsection, however the limit of the variance of the estimates as σ tends to infinity is infinity. Namely, the accuracy of the estimates in a randomized version of the standard algorithm is not practical.

Baba *et al.* [2] proposed a randomized algorithm as an improvement of the algorithm in [1]. In this algorithm, each character is converted into 1 or -1 and the number of the possible functions from Σ to $\{-1, 1\}$ is 2^σ. The upper bound of the variance of the estimates is $(m - c_i)^2/h$.

5.4 Comparison

We compare the algorithm B in Section 4 with the randomized algorithms referred in this section: the four randomized algorithms [1,10,8,9] in Subsection 5.2, the randomized version of the standard algorithm, and the other algorithm [2] in Subsection 5.3.

We focus on the computation time and the variance of the estimates of the score vector. The result of the comparison is summarized in Table 1.

In Table 1, (a) is the range of the functions which convert characters into numbers for FFT, that is, the domain of the elements of numerical vectors. As mentioned in Subsection 5.3, the practical computation time of FFT for real-valued vectors, especially, for vectors of 1, -1, or 0 is short compared with vectors of complex numbers. This leads an improvement of the accuracy of an estimate which is computed in a given time, since the variance is inverse proportion to the number of samples. (c) is the limit of the upper bound of the variance as σ tends to infinity. If the computation time is reduced to be half by using vectors over $\{-1, 1\}$ instead of vectors over $\mathbf{C}$, it compensates for the double variance.

(b) is the upper bound of the variance of the estimates. By Theorem 3, the upper bound of the variance in the algorithm B is explicitly lower than that in the algorithm in [2].

Table 1. A comparison of randomized algorithms by FFT for the problem of string matching with mismatches. (a) is the domain of the elements of numerical vectors for FFT, (b) is the upper bound of the variance of the estimates, (c) is the limit of (b) as σ tends to infinity, and (d) is the size of the population for samples. $\mathbf{C}$ is the set of complex numbers and $\alpha = (m - c_i)^2/h$.

	(a)	(b)	(c)	(d)
ACD01 [1]	$\mathbf{C}$	$\alpha/2$	$\alpha/2$	σ^σ
SY05 [10]	$\mathbf{C}$	$\alpha \cdot \sigma(\sigma-3)/2(\sigma-1)^2$	$\alpha/2$	$\sigma!$
NBIYH05 [8]	$\mathbf{C}$	$\alpha \cdot (\sigma-2)/(2\sigma-1)$	$\alpha/2$	$\sigma - 1 \sim 2\sigma - 2$
NBMH07 [9]	$\mathbf{C}$	$\alpha \cdot (\sigma-3)/2\sigma$	$\alpha/2$	$\sigma - 1$
(Standard)	$\{0, 1\}$	$(\sigma c_i^2 - 1)$	(∞)	σ
BSTIA03 [2]	$\{-1, 1\}$	α	α	2^σ
Proposed	$\{-1, 1\}$	$\alpha \cdot (\sigma-2)/(\sigma-1)$	α	$\sigma - 1 \sim 2\sigma - 3$

(d) is the number of the functions which convert characters into numbers, that is, the size of the population for samples in each randomized algorithms. In the case where the sampling is operated without replacement, the improvement of the variance is obtained notably when the size is small. If we consider the straightforward product for FFT, the lower bound of the size is $\sigma - 1$ [3]. In the algorithm B, the size is $\sigma - 1$ if σ is a power of two.

6 Conclusion

In this paper, we proposed a randomized algorithm by FFT for the problem of string matching with mismatches. The algorithm consists of FFT computations for binary vectors which can be computed faster than the computation for complex numbers. Therefore, an improvement of the variance of the estimates is obtained by speed-up for the computation of FFT. We analyzed the variance of the estimates in the proposed algorithm and compared it with the variances in the existing algorithms. Our future work is some experiments for practical data with specific speed-up algorithms for FFT of binary vectors.

References

1. Atallah, M.J., Chyzak, F., Dumas, P.: A randomized algorithm for approximate string matching. Algorithmica 29(3), 468–486 (2001)
2. Baba, K., Shinohara, A., Takeda, M., Inenaga, S., Arikawa, S.: A note on randomized algorithm for string matching with mismatches. Nordic Journal of Computing 10(1), 2–12 (2003)
3. Baba, K., Tanaka, Y., Nakatoh, T., Shinohara, A.: A generalization of FFT algorithms for string matching. In: Proc. International Symposium on Information Science and Electrical Engineering 2003 (ISEE 2003), pp. 191–194. Kyushu University (2003)
4. Cormen, T.H., Leiserson, C.E., Rivest, R.L.: Introduction to Algorithms, 2nd edn. MIT Press, Cambridge (2001)
5. Crochemore, M., Rytter, W.: Text Algorithms. Oxford University Press, Oxford (1994)
6. Fischer, M.J., Paterson, M.S.: String-matching and other products. Complexity of Computation (SIAM-AMS Proceedings), 113–125 (1974)
7. Gusfield, D.: Algorithms on Strings, Trees, and Sequences. Cambridge University Press, Cambridge (1997)
8. Nakatoh, T., Baba, K., Ikeda, D., Yamada, Y., Hirokawa, S.: An efficient mapping for scores of string matching. Journal of Automata, Languages and Combinatorics 10(5/6), 697–704 (2005)
9. Nakatoh, T., Baba, K., Mori, M., Hirokawa, S.: An optimal mapping for score of string matching with FFT. DBSJ Letters 6(3), 25–28 (2007) (in Japanese)
10. Schoenmeyr, T., Yu-Zhang, D.: FFT-based algorithms for the string matching with mismatches problem. Journal of Algorithms 57, 130–139 (2005)
11. Sorensen, H.V., Jones, D.L., Heideman, M.T., Burrus, C.S.: Real-valued fast Fourier transform algorithms. IEEE Trans. Acoust., Speech, Signal Processing, ASSP 35(6), 849–863 (1987)

Encryption Methods for Restricted Data Limited in Value Range

Yuji Suga

Internet Initiative Japan Inc.
suga@iij.ad.jp

Abstract. For encrypting digital contents such as image data, there is known a secret key encryption method in which a transmitter and a receiver shares a same encrypting key in secret. In case of encrypting a part of image data, it is necessary to cautiously handle standardized format, so as not to generate a encrypted data outside defined value ranges. I propose a new encryption method using a conventional cipher algorithm and introduce conversion rule for each standard such as JPEG 2000 and PNG.

Keywords: JPEG 2000, Copyright protection, Marker codes.

1 Introduction

With recent rapid progress and pervasiveness of computers and networks, digitization is spreading over various information such as character data, image data, audio data etc. While digital information is free from deterioration for example by the lapse of time and can be constantly stored in a complete state, it is easily reproducible and protection of copyright is becoming a serious issue. For this reason, security technologies for copyright protection are rapidly becoming important.

One of the technologies for copyright protection is an "encryption method". For encrypting digital contents such as image data, there is known a common key encryption method such as AES (Advanced Encryption Standard)[1], SNOW2.0[2] and so on.

On the other hand, as a high efficiency encoding method for compressing image data, there is widely employed the JPEG method recommended by ISO and ITU-T as an international standard encoding method for a single static image. The JPEG method is based on a discrete cosine transformation, but is associated with a drawback that a block-shaped distortion is generated when the compression rate is increased. Therefore, in order to meet a requirement for a higher resolution of the image and to realize a higher compression rate, an encoding method utilizing a discrete wavelet transformation, different from the aforementioned discrete cosine transformation, is proposed and is being standardized as JPEG 2000 [3].

A JPEG 2000 encoder is working as the followings. An input image is at first subjected to a sub band decomposition by a discrete wavelet transformation (DWT), and is then quantized.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 284–295, 2010.

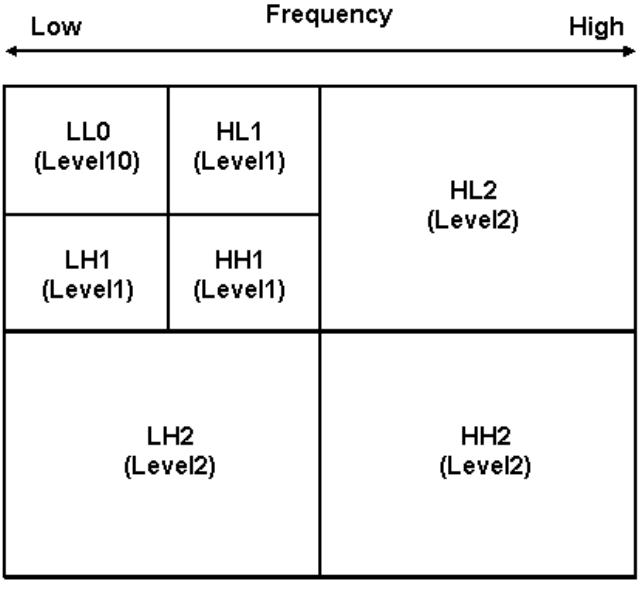


Fig. 1. Sub-band decomposition by DWT in JPEG 2000

Fig.1 shows an example of a sub-band decomposition with a decomposition level of 2 (resolution level = 3), and the resolution levels exist from level 0 to level 2. A coefficient belonging to a lower resolution level contains information of a lower frequency. A quantized wavelet coefficient is encoded by an EBCOT (Embedded Block Coding with Optimized Truncation) algorithm [4]. Such algorithm will be explained in the following five parts of a code block division, a coefficient modeling, an arithmetic encoding and a rate control, a layer formation, and a packet generation.

(1) Code block division. Each sub band is divided into square blocks (for example 64×64), called code blocks. Such code blocks are independently encoded.

(2) Coefficient modeling. For a wavelet coefficient stream of each code block, a coefficient modeling is executed based on a bit plane. In this manner there is generated an embedded code stream in which coefficient bits are arranged in an order of importance. Each of all the bit planes from MSB (Most Significant Bit) to LSB (Least Significant Bit) is decomposed into three subbit planes according to the context. A boundary of each subbit plane is called a truncation point, which constitutes a minimum unit for data discarding later.

(3) Arithmetic encoding and rate control. An adaptive arithmetic encoding is executed on the embedded code stream generated by the coefficient modeling. Thereafter, the arithmetic coded stream is suitably cut off at the truncation

point constituting the boundary of the subbit plane, thereby obtaining a desired bit rate.

(4) Layer formation. In case display is required in succession in plural image qualities, a layer formation of the codes is then executed. Each layer includes a part of the embedded codes of each code block. A higher layer includes a more important portion in the image reproduction.

(5) Packet generation. Each layer is divided into plural units called bodies, and each is given a header information to generate a packet. Each body has information of a corresponding resolution level. Therefore a total number of the generated packets is a product of a number of layers and a number of resolution levels. The header information includes a length of the arithmetic code stream of each code block, a number of subbit planes etc. A final JPEG 2000 code stream is obtained by collecting all the packets and attaching a global header information as shown in Fig.2. However, JPEG 2000 defines that various header information mentioned in the foregoing and the subbit plane constituting a minimum unit of the data division is a size of an integral multiple of a byte.

As explained in the foregoing, digital image data are associated with a security issue, which can be resolved, in case of encryption of the entire image, by the aforementioned encryption methods such as AES. In such case, however, a decrypting operation results in a decryption of the entire image, and a partial protection cannot be obtained. It is nevertheless possible to encrypt a high resolution portion only (level 1 and higher in Fig.1 while leaving the level 0 unencrypted, thereby disclosing the image of level 0 of a low resolution but protecting the entire image of a high resolution. In such case, however, since a portion other than the high resolution portion to be encrypted is in an ordinary code stream of JPEG 2000 format, the AES or SNOW2.0 algorithm cannot be simply applied for encrypting the high resolution portion.

This is because a partial encryption of a JPEG 2000 code stream is associated with a restriction on the marker code[5]. The marker code is a code of a special meaning in the JPEG 2000, and a false marker code, if generated by the encryption, may hinder a proper reproduction. More specifically, in a compressed data portion (body) shown in Fig.2, a marker code has a function similar to an inhibited code of which generation is inhibited code[6].

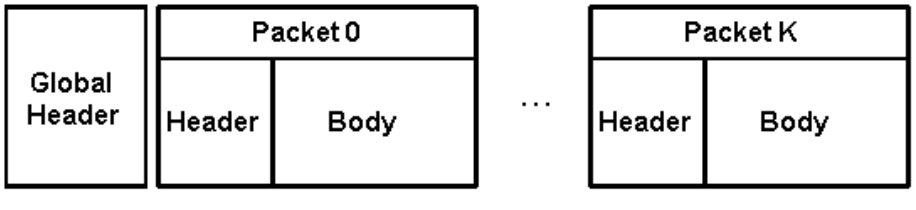


Fig. 2. Conceptual view showing a configuration of a JPEG 2000 stream

In the JPEG 2000, the marker code means a marker having a value of FF90h to FFFFh. The marker is a code storing definition information. It is represented by 2 bytes, of which a first byte is FFh. According to the purpose, the marker is represented by 2-byte code FFxxh. On the other hand, the market segment is constituted of a marker and an ensuing parameter. Four markers only, namely SOC (FF4Fh: start of code stream), EOC (FFD9h: end of code stream), SOD (FF93h: start of data) and EPH (FF92h: end of packet header) are independent codes, and any other marker is a part of the marker segment. Hereafter, the markers and the market segments are collectively called markers. In JPEG 2000, a marker in a range of FF90h to FFFFh is given two particular meanings. Firstly, such marker means a partition in a code stream. It is thus possible to define a position of a packet and a packet header. Secondly, such marker does not exist in the compressed data themselves (body shown in Fig.2. The JPEG 2000 encoder is so designed as not to generate such code. Therefore, in the aforementioned partial encryption of the JPEG 2000 data, it is necessary to avoid generation of such 2-byte marker code of FF90h - FFFFh.

Another data format in which a usable data range is restricted is PNG (Portable Network Graphics). PNG [7] is an image format proposed by a standardizing organization W3C as one of image formats usable in a browser. A file format described by PNG is constituted of a PNG signature and an ensuing group of data clusters called chunks. An example of the PBG signature is 8-byte data 89504E470D0A1A0Ah which are always attached at the beginning of the PNG file.

A chunk is constituted of a stream of four parts, which are a chunk data length (4 bytes), a chunk format code (4 bytes), chunk data (unfixed length) and a CRC (4 bytes). The chunk data length information is 4-byte data indicating a number of bytes of the chunk data area. The chunk format is 4-byte code indicating a format, and data defined according to such format are stored in the chunk data area. The data length of the chunk data area may also be 0. At the end, 4-byte CRC data, calculated as padding data calculated by CRC (Cyclic Redundancy Check) algorithm for the chunk data area, are attached.

For the chunk format code, there can only be used ASCII characters of upper case and lower case (A to Z, a to z). Stated differently, value ranges of 41h to 5Ah and 61h to 7Ah in hexadecimal presentation. Therefore, in case of encrypting a part of the PNG code, it is necessary to cautiously handle such chunk format code, so as not to generate a code outside such value ranges.

2 Proposal Schemes

The format- preserving encryption method [8] has a same motivation mentioned above, however this previous method does not match JPEG 2000 case. Format-preserving encryption must treat data space described in ${Z_2}^n$. On the another hand, representation of restricted JPEG 2000 data can not be described in ${Z_2}^n$ because of complexity of valid data space. So I tried to cover cases such as JPEG 2000s without an approach of format-preserving encryption.

2.1 Encryption Process

Fig.3 shows a flow chart of an encryption process and also there is employed an initial value j = 2.

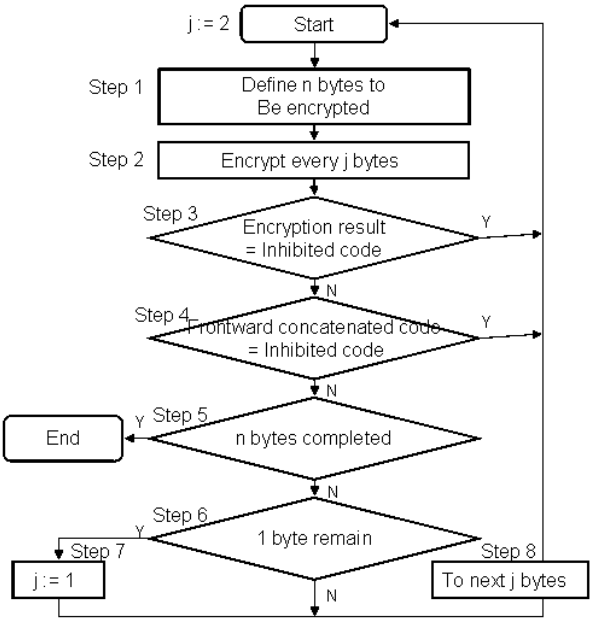


Fig. 3. Encryption process of JPEG2000

At first there are determined n bytes to be encrypted in the JPEG 2000 stream (step 1). There are assumed continuous n bytes in compressed data (data of the body shown in Fig.2) not containing marker codes of FF90h - FFFFh.

Then 2 bytes are taken out from the head of n bytes, and are encrypted (step 2). Such encryption can be achieved by the CTR mode [9] of AES. Then there is discriminated whether the encryption result is a marker code of FF90h - FFFFh (inhibited code) (step 3). In case of an inhibited code, the flow returns to the step 2 for executing the encrypting process again on the encryption result.

Then, in case the encryption result is not an inhibited code, a byte in the latter part of the encryption result positioned in front is connected with a byte in the front part of the current encryption result to form a code (hereinafter called frontward concatenated code) and there is discriminated whether such code is an inhibited code (step 4).

In case it is identified as an inhibited code, the flow returns to the step 2 for repeating the encryption process. This is to prevent presence of an inhibited code even in a frontward or backward concatenated state since the JPEG 2000 stream has a minimum unit of one byte. Since two bytes in the present case are initial ones without a preceding encryption result, they are not an inhibited code

and the flow proceeds to a next step 5. Then there is discriminated whether the second byte is a final n-th byte (step 5). The flow is terminated if it is the n-th byte. If not, there is discriminated whether the second byte is an (n-1)th byte, namely whether there remains one byte (step 6).

In case there remains one byte, there is assumed a value j = 1 (step 7). In the present example, since it is not an n-th byte nor an (n-1)th byte, next two bytes are taken out (step 8). Then the process of the steps 2 to 8 is repeated on such two bytes. For example, in case of n = 4, the second byte corresponds to a 4th byte which is equal to n, the flow is terminated at the step 5. Also in case of n = 5, since the step 6 discriminates that one byte is remaining, there is assumed j = 1 and a next 5th byte alone is taken out (step 7).

In this case, such 1 byte only is encrypted in the step 2. Such 1-byte encryption can be achieved similarly with the CTR mode [9] of AES. In this case, since the encryption result is not a 2-byte code, it is not recognized as an inhibited code in the step 3. Then there is discriminated whether a frontward concatenated code is an inhibited code (step 4). In case the frontward concatenated code is an inhibited code, the flow returns to the step 2 for executing the encryption process again on the encryption result. Then there is discriminated whether such byte is a final n-th byte (step 5). Since n = 5 in the present case, the flow is terminated.

2.2 Decryption Process

Fig.4 shows a flow chart of a decryption process and also there are assumed initial values j = 2 and B = 1.

At first there are determined n bytes to be decrypted in the JPEG 2000 stream (step 1). Such portion to be decrypted is a portion encrypted by the encrypting process shown in Fig.3, and such portion is assumed to be known prior to the decrypting process shown in Fig. 4.

Then there is discriminated whether 1 byte in the latter part of preceding 2 bytes prior to decryption is FF (step 2). In case it is FF, there is assumed a value B = FF (step 3). Since two bytes in the present case are initial ones without a preceding value prior to decryption, B = 0 is retained. Then 2 bytes taken out are decrypted (step 4). Such decryption can be achieved by the aforementioned CFB or OFB mode of AES. In case the result of decryption a marker code of FF90h - FFFFh (inhibited code), the flow returns to the step 4 for executing the decryption process again on the decryption result.

Since the compressed data (body in Fig. 4) constituting the final decryption result contain no inhibited code and a multiple encryption is adopted in case the encryption result in the encryption process shown in Fig. 5 includes an inhibited code, a decryption result including an inhibited code means an encrypted result and requires a decryption again. Then, in case the decryption result is not an inhibited code, there is discriminated whether a code formed by connecting B in front of a byte in the former part of the decryption result (such being called B concatenated code) is an inhibited code (step 6). Since B = 0 in the present case, there is no inhibited code and the flow proceeds to a step 7.

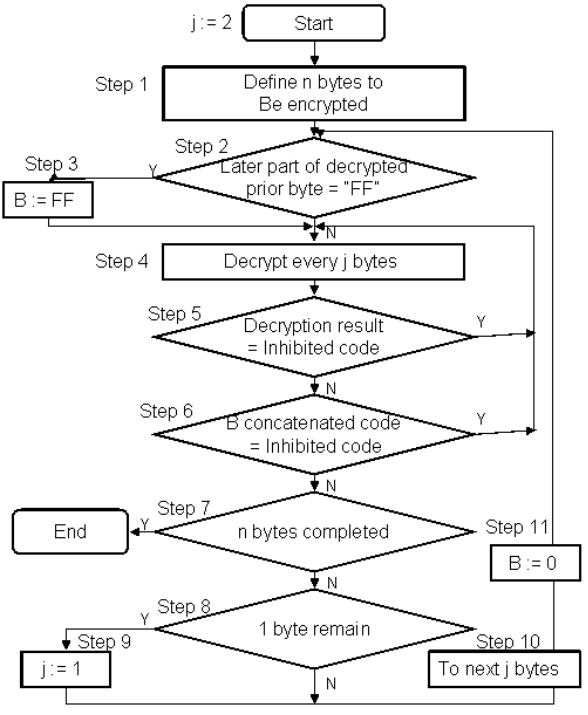


Fig. 4. Decryption process of JPEG2000

Then there is discriminated whether the second byte is a final n-th byte (step 7). The flow is terminated in case it is the n-th byte. If not, there is discriminated whether the second byte is an (n-1)th byte, namely whether there remains one byte (step 8). In case there remains one byte, there is assumed a value j = 1 (step 9). In the present example, since it is not an n-th byte nor an (n-1)th byte, next two bytes are taken out (step 10), and there is assumed a value B = 0 (step 11). Now, let us assume a case where the step 2 in the process of the second cycle identifies a latter byte prior to the decryption in the preceding cycle as FF. This can be confirmed by observing the JPEG 2000 stream stored in the beginning. Therefore, there is assumed B = FF (step 3).

Then two bytes taken out are decrypted (step 4). In case the decryption result is a marker code of FF90h - FFFFh (inhibited code) (step 5), the flow returns to the step 4 in order to execute the decryption process again on such decryption result. In case the decryption result is not an inhibited code, there is discriminated whether a code formed by connecting B in front of a byte in the former part of the decryption result (such being called B concatenated code) is an inhibited code (step 6).

In case the B concatenated code is an inhibited code, the flow returns to the step 4 in order to execute a decryption process again on the decryption result.

This is to prevent presence of an inhibited code even in a frontward or backward concatenated state since the JPEG 2000 stream has a minimum unit of one byte. Then there is discriminated whether the second byte is a final n-th byte (step 7). The flow is terminated if it is the n-th byte. If not, there is discriminated whether the second byte is an (n-1)th byte, namely whether there remains one byte (step 8).

In case there remains one byte, there is assumed a value j = 1 (step 9). For example, in case of n = 4, the second byte corresponds to a 4th byte which is equal to n, the flow is terminated at the step 7. Also in case of n = 5, since the step 8 discriminates that one byte is remaining, there is assumed j = 1 (step 9) and a next 5th byte alone is taken out (step 10). Then the process of the steps 2 to 8 is repeated, and the step 7 identifies n = 5, whereupon the flow is terminated.

3 Examples and Observations

Fig.5 shows an example in which a value range is assumed from 00h to FEh (hexadecimal), and a value out of range is FFh only.

There are shown encryption object data and pseudo random number data to be used in Fig.3. An exclusive logic sum calculation is executed for every byte, to obtain encrypted data. A first byte is processed as follows. Since the encryption object data are 12h while the pseudo random number is E2h, the data after the exclusive logic sum calculation are F0h, which are within the range and are therefore taken as the encrypted data. A second byte is processed similarly to obtain 88. A third byte provides, after the exclusive logic sum calculation, data FFh which are detected as out of range, so that the step4 in Fig.3 executes an exclusive logic sum calculation on FFh and A9h to obtain encrypted data of 56h. As a result, the encryption object data 12345678h provide encrypted data F0885678h.

Fig.6 shows a decryption process for the encryption process shown in Fig.5.

There are shown encrypted data and pseudo random number data to be used in Fig.4. A first byte is processed as follows. Since the encrypted data are F0h while the pseudo random number is E2h, the data after the exclusive logic sum calculation are 12h, which is within the range and are therefore taken as the decrypted data. A second byte is processed similarly to obtain 34h. A third byte provides, after the exclusive logic sum calculation, data FFh which are detected as out of range by step3 (in Fig.4), so that the step 4 (in Fig.4) executes an exclusive logic sum calculation on FFh and A9h to obtain decrypted data of 56h. As a result, the encrypted data F0885678h provides decrypted data 12345678h.

While the previous example has shown a case with one data out of the range, the present process shows that a similar process is possible also in case such data are present in plurality.

Now we consider the case out of range are F0 to FF. A first byte is processed as follows. Since the encryption object data are 12h while the pseudo random number is E2, the data after the exclusive logic sum calculation are F0h, which

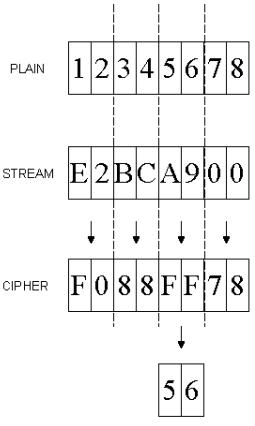


Fig. 5. Example of encryption data

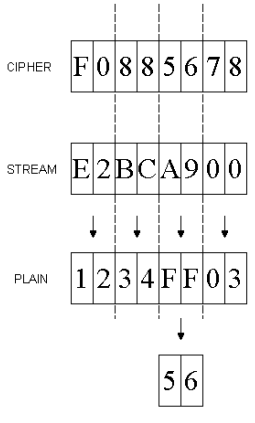


Fig. 6. Example of decryption data

are detected as out of range, so that the step 4 (in Fig.3) executes an exclusive sum calculation on F0h and E2h to obtain encrypted data of 12h. As a result of a similar process, the encryption object data 12345678h provide encrypted data 12885678h.

In case there are many data out of range as in the example of PNG, the encrypted data may show limited scrambled portions in comparison with the data prior to encryption. Therefore, there will be explained a process having a 1-to-1 conversion table from data within the range to data out of the range and executing encryption and decryption utilizing such table.

4 Rules for More Enhanced Processes

The present processed explained a method of executing a process corresponding to a limited value range in JPEG 2000 (data out of range being FF90 to FFFF).

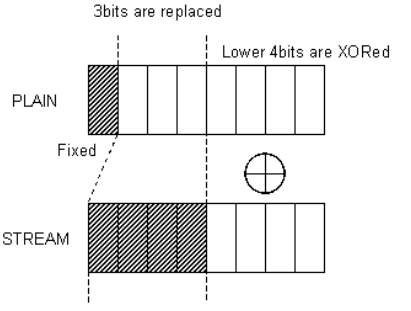


Fig. 7. Conversion method 1

Since the data out of range are from FF90 to FFFF for arbitrary 2-byte data, there can be easily conceived a method of executing encryption for every 2 bytes as in the fifth and sixth embodiments. In the present embodiment, therefore, there will be explained a method of processing every 1 byte.

The aforementioned "data out of range being FF90 to FFFF" can be met in case following rules are satisfied. All the values are 1 byte data, in hexadecimal presentation: rule 1

A) 00 to 8F are converted only to 00 to 8F
B) 90 to FE are converted only to 90 to FE
C) FF is converted only to FF

Fig.7 represents a conversion method satisfying the rule 1, wherein plain data represents bits of 1-byte (8-bit) data processed among the encryption object data. Also stream data represents bits of 1-byte pseudo random number data subjected to an XOR data. The above-mentioned conversion method will be explained with reference to Fig.8.

At first a step 1 enters encryption object data. A step 2 executes a conversion process for 2nd to 4th bits among the input data. In this operation, the values of the 1st to 4th bits of the stream data are utilized, and the conversion is so made as not to change a bit having a value 1. Then a step 3 processes 5th to 8th bits and applies an XOR calculation process on the 5th to 8th bits of the stream data. Then a step 4 discriminates whether data out of range are present, and, if out of range, executes an XOR process as in the step 3. A step 6 discriminates whether all the encryption object data have been processed, and, if not, the flow is transferred to the step 1. The flow is terminated in case the step 6 identifies that the process has been completed.

The above-explained conversion process allows to satisfy the rule 1 and to achieve conversion into the defined value range of JPEG 2000.

In the following there will be explained still another method for conversion so as to meet following rule(rule 2):

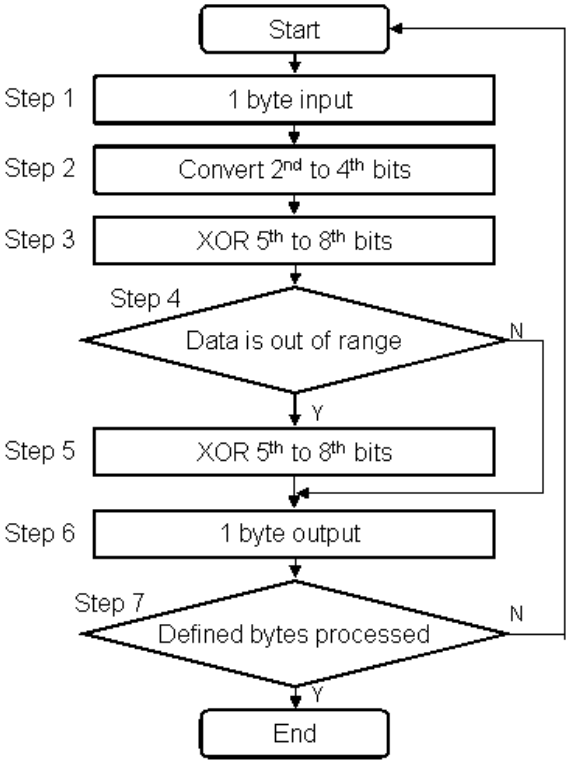


Fig. 8. Encryption process on rule 1

A) 00 to 7F are converted only to 00 to 7F
B) 90 to EF are converted only to 90 to EE
C) upper four bits are converted only from 8 to 8 and from F to F
D) lower four bits are converted only from F to F

Fig.9 represents a conversion method satisfying the rule 2, wherein plain data represents bits of 1-byte (8-bit) data processed among the encryption object data. Also stream data represents bits of 1-byte pseudo random number data subjected to an XORed data.

The above-mentioned conversion method will be explained with reference to Fig.8. At first a step 1 enters encryption object data. Then a step 2 processes 2nd to 4th bits, and applies an XOR process on the 2nd to 4th bits among the stream data. Then a step 3 processes 5th to 8th bits and applies an XOR process on the 5th to 8th bits of the stream data. Then a step 4 discriminates whether data out of range are present, and, if out of range, executes an XOR calculation process as in the step 2 or 3. A step 6 discriminates whether all the encryption object data have been processed, and, if not, the flow is transferred to the step 1.

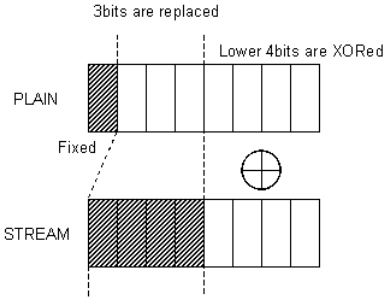


Fig. 9. Conversion method for rule 2

The flow is terminated in case the step 6 identifies that the process has been completed. The above-explained conversion process allows to satisfy the rule 2 and to achieve conversion into the defined value range of JPEG 2000.

5 Conclusion

This paper proposed new encryption/decryption schemes about restricted image formats, for example especially JPEG2000 and PNG. This proposal solves the problem that JPEG 2000 decoder can not process due to the restricted data. And I also introduced new rules for enhanced proposals especially JPEG 2000. In the future I research whether it is possible to apply to other formats and estimate calculation costs.

References

1. NIST Federal Information Processing Standards Publication 197, Advanced Encryption Standard, AES (2001)
2. Ekdahl, P., Johansson, T.: A new version of the stream cipher SNOW. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 47–61. Springer, Heidelberg (2003)
3. ISO/IEC 15444-1:2004 — ITU-T Rec. T.800, JPEG 2000, image coding system: Core coding system (2000)
4. Taubinan, D.: Eiiibcclded Block Codirig in JPEG-2000. In: Proc. of IEEE International Conference on Image Processing, vol. 2, pp. 33–36 (2000)
5. ISO/IEC JTC 1/SC 29/WG 1 N 3412 (2004)
6. Iwamura, K., Hayashi, J.: Encryption Scheme without generating marker codes for JPEG 2000 image. The Transactions of the Institute of Electronics, Information and Communication Engineers J90-A(11), 839–850 (2007)
7. ISO/IEC 15948:2003, Portable Network Graphics (PNG): Functional specification
8. Bellare, M., Ristenpart, T.: Format-Preserving Encryption. In: Rijmen, V. (ed.) SAC 2009. LNCS, vol. 5867, pp. 295–312. Springer, Heidelberg (2009)
9. NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation (2001)

The Research for Spatial Role-Based Access Control Model

Zhiwen Zou, Changqian Chen, Shiguang Ju, and Jiming Chen

School of Computer Science and Telecommunications Engineering,
Jiangsu University, Zhenjiang, Jiangsu, PR. China
ZZW_YJ@126.com

Abstract. The Spatial Role-Based Access Control (SRBAC) model was discussed in this paper. Firstly, the formal definition of SRBAC Model was given; then the region coverage constraint of spatial object, duration constraint of spatial object, various spatial object separations of duty constraints and spatial object cardinality constraint of role activation were researched; after extending the traditional session, the strategy of eliminating the conflictive session was presented; Finally, the role hierarchy has been discussed under the spatial environment. Combined with practical application, the theory of secure DBMS was optimized and afforded to build the stricter system.

Keywords: Access control model; spatial character; constraint; session; hierarchy.

1 Introduction

The emergence of Role-Based Access Control makes a great convenience to system permission administration [1]. A great many researchers have discussed about how to apply RBAC model to multilevel security system, including that how to use RBAC to analogize DAC and MAC [2], and make use of RBAC [3] on condition that multilevel system core model is unchanged [4]. Permission was authorized to role but not to user in RBAC. The user will possess the permission of the role if the role is authorized to it. Special rules are enforced in RBAC when the permission is authorized to roles, roles to the users or users activate a role. The utility of RBAC model not only facilitate the administration but also lower the complication, costs and probability of errors. As a result, RBAC has developed rapidly in recent years.

Currently, some influential models have been proposed. For instance, the model RBAC96 proposed by R.Sandhu which is described systemically and comprehensively is accepted wide. Four concept models are defined in RBAC96 model, role administration is discussed as well. However, division and set up are not mentioned in real system development for failing to recognize the role concept systemically. The model RBAC2000 [5] developed by The National Institute of Standards and Technology study group unified the cognizance to RBAC. According to expanding the model RBAC2000, the Temporal Role-Based Access Control model is put forward which include time extent constraint conception and time length constraint conception.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 296–308, 2010.

Spatial Role-based Access Control is put forward in references [6, 7] which intended as a role that is automatically activated when the user is in a given position. The spatial granularity of the position is thus fixed while the space is rigidly structured. This extension of RBAC model is targeted to wireless network applications and concisely proposed segregation of duty constraint and role hierarchies with spatial characters. But the rule of role inherit, constraint and session state with spatial characters is not discussed in detail. IRay and LYu proposed an access control model based location [8, 9], the model just consider the relation between different components and location of RBAC model, but did not consider the influence of environment to access control. Elisa Bertino proposed GEO-RBAC model [10], which apply to deal with permission control between space and information based on geographical position according to expending traditional RBAC model. In this model, objects, geographical position of users and roles constraint by geographical position are explained by spatial entity. Roles of users are activated rest with the geographical position of users. At the same time, in order to advance flexibility and reusability of the model, the concept of role schema is introduced to GEO-RBAC model. It includes the name of role, the type of available scope of role space and the granularity of logical position and so on. But insufficient suggestions are argued to the spatial constraint rule of roles. Zhang Hong introduced the conception of spatial role and integrated spatial context to roles [11], according the current location of user to identify which role is effectual in session and establish the spatial duties isolation restraint, location-based cardinal number restraint and location-based time sequence restraint for restrained SC-RBAC model. XCui proposed an Ex-RBAC model [12] through addition of identity restraint and space-time restraint in mobile cooperation system. But, these models did not consider the influence of mobile calculation to access control. In a word, some proposed models have considered the spatial factor to access control, but the influence of roles in mobile calculation environment to access control was not analyzed in detail for current proposed access control models.

In spatial environment, the permission usage of role is restricted by the scope of role. The operation permission to object is authorized only when the current location of user is in the spatial scope of the acted role. The permission authorization and cancellation must be according to the location of object and users when system is making access control decision. Reasonable improvement was needed when the current role-based access control model applying to access control of spatial data.

Accordingly, taking into account the above factors, we mainly research the character of SBRAC model and advance the formal definition of SRBAC model. At the same time, we have analyzed four kinds of constraint of RBAC model in different spatial environments, discussed different kind of conflicts of session and how to deal with it and advanced the rules of role inheritor .Then the ability of security description of SRBAC model will be improved.

2 SRBAC Model

SRBAC model is an extension of the traditional RBAC96. In this model, a role at different spatial locations has different permissions.

Definition 1: formal definition of SRBAC Model

$U = \{u_1, u_2, ..., u_n\}$ is a set of all users;

$R = \{r_1, r_2, ..., r_n\}$ is a set of all the roles;

$Ob = \{ob_1, ob_2, ..., ob_k\}$ is a set of all the objects;

$Op = \{op_1, op_2, ..., op_k\}$ is a set of all operations;

$S = \{s_1, s_2, ..., s_p\}$ is a set of all sessions;

$P = 2^{Op \times Ob}$ is a set of all permissions;

$LOC = \{LOC_1, LOC_2, ..., LOC_n\}$ is the set of all spatial location.

$UA \subseteq U \times LOC \times R$ is many-to-many mapping from the user set to the role set, which denotes that users have been given the role in some location;

$PA \subseteq P \times LOC \times R$ is many-to-many mapping from the permission set to the role set, which denotes that roles have been given the permission in some location;

$RH \subseteq R \times R \times LOC$ is a partial order on the role set, known as the hierarchy. If $(r_i, r_j) \in RH$, defined as $r_i \overset{\succ}{_{(lOC)}} r_j$, which denotes that r_i inherits permission of r_j in spatial location LOC.

$S = < U, R, UA, PA, C, ChangePosition, Op >$, session S refers to an interlocution between the user and the system. Session is described by 7 elements. Here in the session, U is defined as a user, R is defined as a role, UA is defined as mapping relations between the user and the role, PA is defined as mapping relations between the role and the permission, C is defined as the abided rules during the runtime. ChangePosition is the spatial location with session state changing. $Op \subseteq R \times S$, is a series of operation during the session. Here we only give some operations briefly in this paper.

Op1. authorized (*r*, *LOC*): authorize *r* role in the spatial position *LOC*.
Op2. assign_user (*u*, *r*, *LOC*): assign *r* role to user *u* in the spatial position *LOC*.
Op3.assign_perm (*r*, *p*, *LOC*): assign permission *p* to role *r* in the spatial position *LOC*.
Op4. get_role (*u*, *r*, *LOC*): activate role *r* of user u in the spatial position *LOC*.
Op5. get_perm(*u*, *p*, *LOC*): user *u* get permission *p* in the spatial position *LOC*.
Op6. get_perm_role (*p*, *r*, *LOC*): role *r* get permission *p* in the spatial position *LOC*.
Op7. session_role(*u*,*s*,*LOC*):return relational role of user *u* in session *s* in the spatial position *LOC*.
Op8. session_perm(*u*,*s*,*LOC*): return relational permission of user *u* in session *s* in the spatial position *LOC*.

Definition 2: spatial left relationship

There are two spatial location $L_i(X_i, Y_i) \in LOC$, $L_j(X_j, Y_j) \in LOC$, if $X_i < X_j$, define as L_i is in the left of L_j, recorded as $L_i < L_j$.

Definition 3: spatial region

$LS = \{< L_i, L_j > | L_i, L_j \in LOC, i < j\}$ can be thought of the spatial region defined by $< L_i, L_j >$. Regional character of spatial objects is the minimum bordering rectangle (MBR), $LOCSet = 2^{LS}$ is a set be composed of spatial region.

At the same time, we can provide a role authority state or non- authorized state. Users can be only assigned a role, and this role must be authority state, then the user can activate this role. When the role is in a non-authorized state, it could not be activated. In the system each session has a priority, and the priority is marked with p. $(p, \leq)$ is a partial order.

3 Constraint of SRBAC Model

In our SRBAC model, a rule library with spatial constraint is defined. In the rule library, constraint is divided into four kinds, such as the region coverage constraint of spatial object, duration constraint of spatial object, various spatial object separations of duty constraints and spatial object cardinality constraint of role activation. The four kinds of constraint reflect the permission control rules of a role in spatial area. Administrators may activate or forbid these constraints according to the necessary of safety.

The region coverage constraint of spatial object is used to decide if session can be set up between users in some special scope of spatial region. The session could assign role to users, distribute permission to role and change the state of role.

Duration constraint of spatial object is used to decide the size of spatial region where users are allowed to set up session. The session could assign role to users, distribute permission to role and change the state of role. The originate position of the region coverage constraint of spatial object is known, but the originate position of duration constraint of spatial object is unknown. Its originate position is where users set up the session.

Spatial object cardinality constraint of role activation is composed by Constraints on the maximum number of the roles (MAXr) and Constraints on the maximum number of user-role assignment set (MAXur). MAXr is confined to a special spatial region, which is the upper limit of activation cardinality for one role, no matter whether the users are in different sessions or the role is activated by different users. MAXur are confined to a special spatial region, which is the upper limit of activation cardinality for one role by a special user, no matter whether the user is in different sessions. The upper limit of activation cardinality is definite for the same role in a special spatial region, but indefinite for the same role activated by different users in a special spatial region.

Various spatial object separations of duty constraints are applied to control the conflict roles used in same spatial areas and the same roles used in conflict spatial areas. It is mainly used to limit the permission of users. In traditional RBAC model, Separations of Duty (SoD) constraints are introduced to prevent conflicts of interest arising when a single individual can simultaneously perform sensitive tasks requiring the use of mutually exclusive duties. The Separation of Duty is very importantly to protect information security. We have expanded the traditional SoD in SRBAC, defined as

static spatial separation of duty (SSSoD) and dynamic spatial separation of duty (DSSoD). For example, consider two roles, Doctor and Nurse defined at a common extent representing a hospital. It seems reasonable to assume that an individual should not be authorized to play the role of Doctor in two different locations, i.e. hospitals; similarly, one should not be authorized to play the roles of Doctor and Nurse in the same location. In the latter case, we observe that roles become incompatible when the extents of Doctor and Nurse satisfy a precise topological relationship, specifically their extents coincide.

In SRBAC model, constraint has two states of static or dynamic. If the constraint is dynamic, we have to identity the state of constraint is activated or available. The role is inoperative until it is activated and available. In order to maintain the security of system, administrator has a ability for changing the role into unavailable state and prohibiting user access them, while administrator find some roles are used by unsafe users. Dynamic constraint set runs in active states, just like traditional dynamic constraint of duty segregation, to avoid conflict when users in the same session.

A session is created in a spatial region by users. System will trigger the constraints and control the session working automatically, if some constraints related to this session exist. If they do not exist, the session will continuously work until end or disrupted by other sessions.

4 Session of SRBAC Model

Assume that there is a session set $S = \prec S(LOC_1), S(LOC_2), ...S(LOC_t), ... \succ$, $S(LOC_t) \in S$, in the spatial position LOC_t of the system. Different sessions may bring conflict in the system. For example, a session assign role *r* to the user and another session abolish the assigned role of user *r*, thus the two sessions fall across a conflict.

4.1 Category of Conflictive Session

According to table1, there are two category of conflictive session

- similar session conflicts (type1). The character of these sessions is having the same kind of behavior for same role. For example, a session change the role from the authorize state into non-authorized state, while the other change the role from the non-authorize state into authorized state.
- different session conflicts (type2). The character of these sessions is having different behaviors for same role. For example, a session activate a role, while the other change the role from the authorize state into non-authorized state (the role in non-authorized state could not be activated).

4.2 Strategy of Eliminating the Conflictive Session

Definition 4: strategy of eliminating the conflictive session

S is a session set, $p : S$ is a session whose priority is *p*, if priority $q : Conf(S)$ of the session meets the following conditions, the session *q* can obstruct session *p*.

Table 1. Category of conflictive session

Type	S_1	S_2=Conf(S_1)	Conditions
type1	authorized(r_1,*LOC*)	unauthorized(r_2,*LOC*)	$r_1 = r_2$
type1	assign_user(u_1,r_1,*LOC*)	unassign_user(u_2,r_2,*LOC*)	$r_1 = r_2 \wedge u_1 = u_2$
type1	assign_perm(p_1,r_1,*LOC*)	unassign_perm(p_2,r_2,*LOC*)	$r_1 = r_2 \wedge p_1 = p_2$
type2	get_role(u,r_1,*LOC*)	unauthorized(r_1,*LOC*)	$r_1 = r_2$
type2	get_role(u_1,r_1,*LOC*)	unassign_user(u_2,r_2,*LOC*)	$r_1 = r_2 \wedge u_1 = u_2$

- if $p:S$ and $q:Conf(S)$ are type1 of conflictive sessions, and S belongs to S_1 of Table1, $p \le q$ or S belongs to S_2 of Table1, $q>p$.
- if $p:S$ and $q:Conf(S)$ are type2 of conflictive sessions, and S belongs to S_1 of Table1.
- having associated constraints , users are prohibited to create the session *S*.

For the conflictive sessions, the session with high priority obstruct session with low priority. If two sessions have the same priority, take "no" priority principle. At the same time, if type1 and type2 sessions exist at the same time, we first eliminate type1 of the session. Because activating the role is dependent on whether the user has assigned to the role and the state of the role.

4.3 Example

Set a session: S = (H: S_1 (authorized (r_1, *LOC*)), H: S_2 (unauthorized (r_1, *LOC*)), *VH*: S_3 (authorized (r_2, *LOC*)), H: S_4 (unauthorized (r_2, *LOC*)) , *VH*: S_5 (assign_user (u_1, r_2, *LOC*)), H: S_6 (assign_user (u_2, r_2, *LOC*), open constraint *c*)), *VH* has a priority level higher than H.Dealling with type1 and type2 conflict, we will get *Nonblock* = (H: S_2 (unauthorized (r_1, *LOC*)), *VH*: S_3 (authorized (r_2, *LOC*)), *VH*: S_5 (assign_user (u_1, r_2, *LOC*)), H: S_6 (assign_user (u_2, r_2, *LOC*)), the open constraint *c*), constraint *c* suggests that r_2 can be activated only once. Because security S_6 is lower than S_5, thus S_6 is obstructed. According to the above rules, the final session sequence is (H: S_2 (unauthorized (r_1, *LOC*)), *VH*: S_3 (authorized (r_2, *LOC*)), *VH*: S_5 (assign_user (u_1, r_2, *LOC*))).

4.4 Changes of Session State and Scheduled Strategy

In the RBAC model with spatial character, session plays an important part in the study of spatial character on SRBAC model. The spatial character of the whole model focuses on the spatial character of the session.

Definition 5: Function expansion of SRBAC model

start: $LS \to LOC : start(Li, Lj) = Li$

end: $LS \to LOC : end(Li, Lj) = Lj$

in_range: $LOC \times LS \to \{true, false\} : in\_range(L,(Li, Lj)) = (L \ge Li) \wedge (L \le Lj)$

Function can expand with the needs of users. In SRBAC model, the session may not satisfy the spatial constraints, but with the user's spatial location change, the session is likely to satisfy the definition rules of the spatial constraints. Therefore, whenever the user changes its location, the system should judge session state legitimacy, but obvious flaw with this approach is that when the rules are so many that it is difficult to guarantee efficiency, and this is unrealistic. Thus we present algorithm to solve this problem.

Algorithm: Calculation spatial position of the session state changes
Input: Session S, activate the space regional constraints $LOCSet$, $curt\_pos$ can be thought as the current spatial location of users
Output: The spatial location scp causing the session state changes
Begin
If there is no spatial constraints
$scp = \infty$
else if $\exists LS \in LOCSet \quad \wedge \quad in\_range(curt\_pos, LS)$
scp= end(LS)
else
find a spatial region constraints LS From $LOCSet$, satisfy that $curt\_pos(start(LS) \wedge \forall LSi \in LOCSet \wedge (start(LS) - curt\_pos) \leq (start(LSi) - curt\_pos)$
scp = start(LS)
Endif
Endif
End

Scp is the spatial location what causes the session state change.

When we compute the spatial position at the first time, we should guarantee that relative spatial constraint of the session is activated if the state of session changes. we can directly compute the spatial position when the state of session changed.

Session has four states in its lifecycle: operational, obstructed, error and close. It can be changed from one state to other state. The change is on the basis of decision to constraint rules. User creates a session in a spatial area, if without relative constraint, and it will run until to the end or other sessions stop it. If the session has relative constraint, system will trigger it automatically and control the running of session. When session satisfies constraint of relative characters, it will be interposed into operational queue, otherwise into obstructed queue. If session violates the system security policy, it should be terminated.

5 Hierarchy of SRBAC Model

Firstly, we define four rules:

$\cdot\, assign\_perm(p, r, LOC) \rightarrow get\_perm\_role(p, r, LOC)$

In spatial position LOC, p is assigned to role r, in this case we can get the permission p through r.

$\cdot\, assign\_user(u, r, LOC) \rightarrow get\_role(u, r, LOC)$

In spatial position *LOC*, *r* is assigned to user *u*, we can get the role *r* through *u*.

$$\cdot\ get\_role(u,r,LOC) \wedge get\_perm\_role(p,r,LOC) \rightarrow get\_perm(u,p,LOC)$$

In spatial position *LOC*, *r* is assigned to user *u*, *p* is assigned to role *r*, in this case *u* can get permission through role *r*.

$$\cdot\ get\_role(u,r,LOC) \wedge get\_perm\_role(p,r,LOC) \rightarrow \text{session}\_perm(u,p,LOC)$$

In spatial position *LOC*, *u* creates session to activate *t* role *r*, *p* is assigned to *r*. In this case s created by user *u* can get the permission *p*.

In reference [13], Sandhu divides role hierarchy into permission hierarchy and activation hierarchy, activation hierarchy is the extent of permission hierarchy.

·Permission hierarchy ($\geq$): Child can inherit permission of parents, but user can not activate the role of parents.

·Activation hierarchy ($\succ$):Child can not inherit permission of parents directly, but the user assigned to role of child can activate parents and acquire permission of parents.

In spatial environment, parents and child can possess different state in the same spatial area. Thus, we divide hierarchy into incompact hierarchy and strict hierarchy in spatial environment. Accordingly, we can implement the rule of minimum privilege preferably.

·(incompact permission hierarchy) $r_i \geq_{(W,LOC)} r_j$, if r_i is in a authorized state in spatial position *LOC*, r_i can inherit the permission of r_j regardless of authorized state of r_j.

$$\forall p(x \geq_{(W,LOC)} y) \wedge authorized(x,LOC) \wedge get\_perm(p,y,LOC) \rightarrow get\_per(p,x,LOC)$$

·(strict permission hierarchy) $r_i \geq_{(S,LOC)} r_j$, r_i can inherit the permission of r_j in conditions of r_i and r_j are in a authorized state in spatial position *LOC*.

$$\forall p(x \geq_{(S,LOC)} y) \wedge authorized(x,LOC) \wedge authorized(y,LOC)$$
$$\wedge get\_perm(p,y,LOC) \rightarrow get\_perm(p,x,LOC)$$

·(incompact activated hierarchy) $r_i \succ_{(W,LOC)} r_j$, if r_j is in a authorized state in spatial position *LOC*, user can activate role r_j on condition that r_i is assigned to the user.

$$\forall u(x \succ_{(W,LOC)} y) \wedge authorized(y,LOC) \wedge session\_role(u,s,x,LOC)$$
$$\rightarrow session\_role(u,s,y,LOC)$$

·(strict activated hierarchy) $r_i \succ_{(S,LOC)} r_j$, if r_i and r_j are in a authorized state, user can activate the role r_j on condition that r_i is assigned to the user.

$$\forall u(x \succ_{(S,LOC)} y) \wedge authorized(x,LOC) \wedge authorized(y,LOC)$$
$$\wedge session\_role(u,s,x,LOC) \rightarrow session\_role(u,s,y,LOC)$$

In Fig.1., Fig.2., the role of super administrator is in authorized state in area1. But administrator1 is in authorized state in area2, and administrator2 is in authorized state

in area3. Fig.1. indicate incompact permission hierarchy, user that assigned to super administrator can inherit the permission of administrator1 and administrator2 in area1. Fig.2. indicates the strict permission hierarchy. Users assigned to super administrator can not inherit the permission of administrator1 and administrator2 in area1.

In Fig.3., super administrator is in authorized state in any area. Administrator1 and administrator2 are in authorized state in area1. Owing to Fig.3. indicate incompact activated hierarchy, users assigned to super administrator can activate administrator1 and administrator2 in area1.

In Fig.4., super administrator is in authorized state in area1 and area2. Administrator1 is in authorized state in area1 but administrator2 in area2. Owing to Fig.4. indicate strict activated hierarchy, users assigned to super administrator can activate administrator1 in area1 and administrator2 in area2.

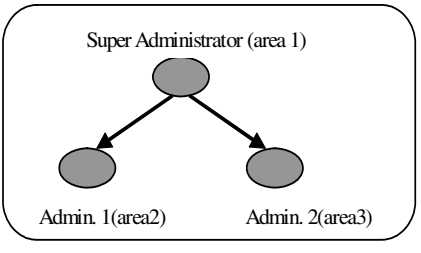


Fig. 1. Incompact permission hierarchy

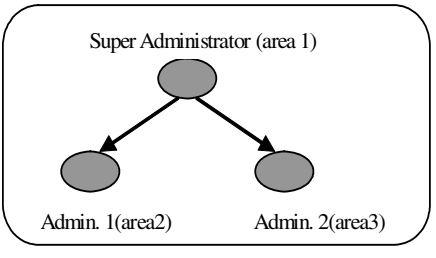


Fig. 2. Strict permission hierarchy

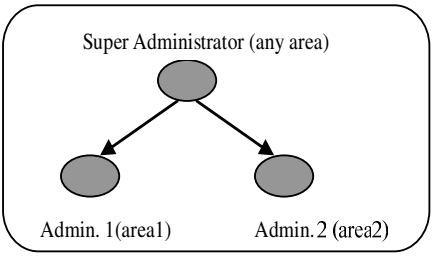


Fig. 3. Incompact activated hierarchy

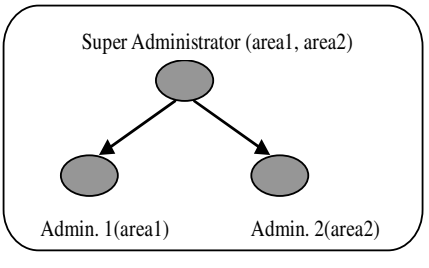


Fig. 4. Strict activated hierarchy

6 Application

SecVista is a secure spatial DBMS which developed by ourselves. The objects of SecVista are mainly used to deal with the information of substance in the surface of earth. SecVista has such secure functions, including user identity authentication, discretionary access control, mandatory access control, audited tracing and separation of the executive, legislative and judicial powers. Thanks to the ceaseless development of spatial DB and its huge size, a high criterion is applied to the template of secure management. Taking into account the above factors, SRBAC model is applied to SecVista.

Accordingly, control subsystems of SRBAC model of the spatial DBMS include RBAC management services, identity authentication services, session management services, access decision-making services and constraint management services. They are supported by RBAC database. The relationship among them is shown as Fig.5, and lines indicate the flow of date.

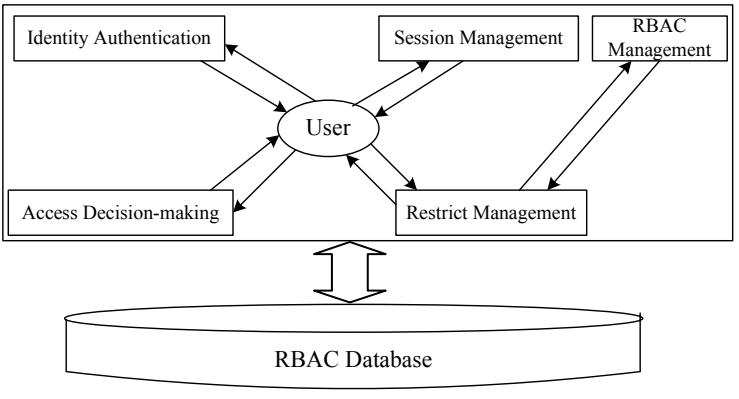


Fig. 5. System Architecture of access control subsystem

RBAC system management module is in charge of the management of RBAC database, its duty include change the number of user and role, the assignment of users and roles, the permission of role and define the relationship among roles. Every operation has relative parameters and premise conditions, and makes DB changed dynamically. System administrators make use of the module initialize RBAC database and maintain it.

When user submits a request that access some resources, the relative information of access control is filtered by access request policy decision. Such as activated roles of user, accessed subjects, requested operation and so on. According to selecting RBAC database, the requests can be judged accepting or not and return the result to users.

When an authorized request was submitted by user, constraint management services will be started to judge the grant whether produces conflict among constraints. If it produced the conflict, the authorized request will be rejected. Otherwise, accept the request and record it.

Session management module and RBAC database administer sessions cooperatively. Including create a session, cancel a session and administer the activated roles. The module has to use relative tables: users table, roles table, dynamically roles table, session table, activating roles table.

In table2, role constraints with spatial character exist in SecVista system. Constraint1 is the region coverage constraint, a1 indicate the administrator is in the state of authorized in office, but unauthorized at home. And b1 indicate that Wang can be assigned to administrator in office, but only role of inquirer at home. Constraint2 is Duration constraint of spatial object, and Li is assigned to administrator in office but his territory is only one hundred square meters. Constraint3 is spatial object cardinality constraint of role activation, a3 indicate the number of users who can activate the

number of administrator is less than five in office, and Li can be activated only one time. For instance, from constraint b1, Wang can select the information of rivers and communication tower in office(Fig.6.), but only the information of rivers is selectable at home(Fig.7.).

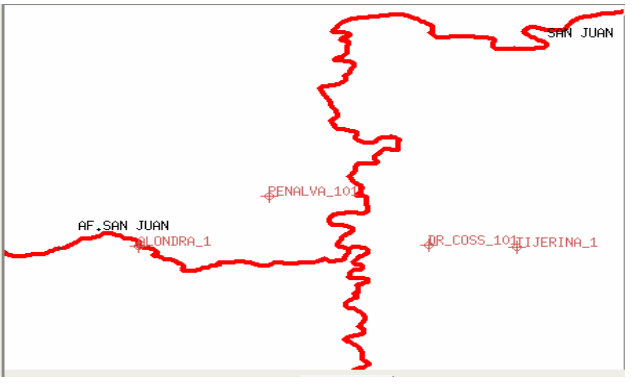


Fig. 6. Selected information in office

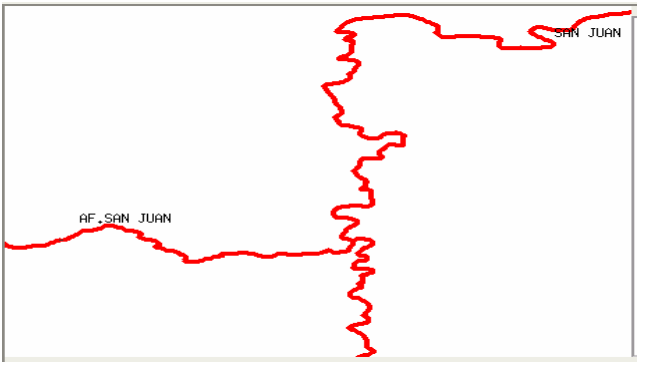


Fig. 7. Selected information at home

Table 2. Role constraints with spatial character

Constraint1	a1	(office, unauthorized(administrator))	(home, unauthorized(administrator))
Constraint1	b1	(office, assign_user(Wang,administrator))	(home, assign_user(Wang,inquirer))
Constraint2	a2	(office, assign_user(Li, administrator))	
Constraint2	b2	(100sq.m., assign_user(Li, administrator))	
Constraint3	a3	(office, 5, active(administrator))	
Constraint3	b3	(office, 1, active(Li, administrator))	

7 Conclusion

SRBAC is the expansion of spatial character in RBAC96. SRBAC model with spatial character has more comprehensive, more specific description of the security. SRBAC has expanded traditional constraints, session and system status in the fact of space and solved the problem of the spatial constraints and session state change. However, spatial environment is simulated just with minimal bounding rectangle in this paper. We should make further research as the complexity of the residential space and the mobility of users. On the other hand, how to implement safety constraints and security strategy and ensure good system access performance is the question we should continue to pay attention to for in the current existing in the realization of inferior efficiency as a safe access model to SRBAC model.

Acknowledgments

This work was supported by nature science foundation of China (no.60773049), Jiangsu project innovation for PHD candidates (CX07B_125z), Jiangsu small- and medium-sized enterprises technique innovation foundation (BC2008140) and Zhenjiang social development foundation (SH2006056, SH2008028).

References

1. Sandhu, R.S., Conye, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE computer 29(2), 38–47 (1996)
2. Osborn, S.L., Sandhu, R., Munawer, Q.: Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. ACM Trans Information and System Security 3(2) (February 2000)
3. Richard Kuhn, D.: Role based access control on MLS systems without kernel changes. In: Proc. of the third ACM Workshop on Role-Based Access Control , Fairfax, Virginia, United States, October 22-23, pp. 25–32 (1998)
4. Osborn, S.: Mandatory access control and role-based access control revisited. In: Proc of the Second ACM Workshop on Role-Based Access Control, Fairfa, Virginia, United States, November 06-07, pp. 31–40 (1997)
5. Ferraiolo, D.F., Sandhu, R., Gavrila, S.: Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security 4(3), 224–274 (2001)
6. Hansen, F., Oleshchuk, V.: Spatial Role-Based Access Control Model for Wireless Networks. IEEE, Los Alamitos (2003)
7. Hansen, F., Oleshchuk, V.: SRBAC: a spatial role-based access control model for mobile systems. In: Proceedings of the 7th Nordic Workshop on Secure IT Systems, Norway (2003)
8. Ray, I., Yu, L.: Short paper: towards a location-aware role-based access control model. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 234–236. IEEE Computer Society, Athens (2005)
9. Ray, I., Kumar, M., Yu, L.: LRBAC: A location-aware role-based access control model. In: Bagchi, A., Atluri, V. (eds.) ICISS 2006. LNCS, vol. 4332, pp. 147–161. Springer, Kolkata (2006)

10. Bertino, E., Catania, B., Damiani, M.L., Perlasca, P.: GEO-RBAC: a spatially aware RBAC. In: SACMAT 2005, pp. 29–37 (2005)
11. Hong, Z., Yeping, H., Zhiguo, S.: A formal model for access control with supporting spatial context. Science in China Series F: Information Sciences 50, 419–439 (2007) (In Chinese)
12. Cui, X., Chen, Y., Gu, J.: Ex-RBAC: An extended role based access control model for location-aware mobile collaboration system. In: Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP 2007), pp. 36–41. IEEE Computer Society, Silicon Valley (2007)
13. Sandhu, R.: Role activation hierarchies. In: Proceddings of 2rd Acm Workshop on Role-based Access Control, Fairfax, Virginia, October 22-23, pp. 65–79 (1998)

A Bidirectional Heuristic Search Technique for Web Service Composition

Nilesh Ukey[1], Rajdeep Niyogi[1], Alfredo Milani[2], and Kuldip Singh[1]

[1] Department of Electronics and Computer Engineering,
Indian Institute of Technology Roorkee, India
{tilluuec,rajdpfec,ksconfcn}@iitr.ernet.in
[2] Department of Mathematics and Computer Science,
University of Perugia, Italy
milani@unipg.it

Abstract. Automatic web services composition has recently received considerable attention from researchers in different fields. In this paper we propose a model based on web service dependency graph and a bidirectional heuristic search algorithm to find composite web services. The proposed algorithm is based on a new domain independent heuristic. Experiments on different types of dependency graphs of varying sizes and number of web services show promising results for the service composition model when compared to state-of-the-art search algorithms. The proposed dependency graph based composition model is, however, not limited to traditional web services but it can be extended to more general frameworks of collective systems where a global intelligent behavior emerges by a plurality of agents which interact composing different actions, services, or resources.

Keywords: Web service composition, dependency graph, heuristic search algorithm.

1 Introduction

The World Wide Web has gradually moved from a human-centric web to an application-centric web i.e., from web pages to web services. A web service is defined by the W3C as a software method together with protocols designed to support interoperable machine-to-machine interaction over a network. The increasing number of available web services over the past few years has led to the development of new web services and complex applications by composing existing web services. The interest of efficient automatic composition mechanisms is motivated by the opportunity and the flexibility offered by a new generation of business applications, which can be dynamically reconfigured depending upon costs, performances, and functionalities offered by the services available on the "cloud" over time.

Web service composition means providing new services that do not exist on their own, using only the existing web services. Therefore, in order to have a more complex service, we can use some semantically related simpler web services and integrate them in such a way that the whole set provides the desired service. In essence, web

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 309–320, 2010.

service composition can be viewed as the problem where the output parameters of a web service can be used as the input parameters of another web service.

Methodologies of web services composition and the related issues has been discussed at length by Dustdar and Schreiner [1] and by other researchers [2,3]. However, the performance time of these schemes is still a matter of concern due to the large number of web services. There are web service specification languages that specify semantic properties of web services. We use these semantic properties to create an abstract model of web service dependencies based on the notion of dependency graph introduced in [4,5]. We develop a heuristic search algorithm for composite web service generation.

It is worth noticing that besides the W3C standard web services, the dependency based composition model can be applied to a great variety of more general services and resources which are available on the web. Examples of more general services/resources are: human oriented services provided by web sites, such as retrieval engines, automatic translators, query services that can be invoked only by means of wrappers [6] or by API which are often not W3C standard web services (see RSS feeds or Google API for example); complex resources such as maps, vocabularies, video and multimedia which are available directly on the web or as a result of services invocation and which in turn can be given as input to other services; finally collective systems i.e., for example social networks, where a large number of users/agents make available resources and human driven services, such as rating, tagging etc., which can be composed in order to realize some complex behavior (e.g., ask a user to rate a story written by another one).

The rest of the paper is organized as follows. Section 2 gives a model of web service dependencies based on dependency graph. In Section 3 a bidirectional heuristic search algorithm is discussed in detail along with the proposed heuristic. Section 4 discusses the results of execution of our algorithm and displays the effectiveness of the algorithm. We conclude with a brief discussion in Section 5.

2 A Model of Web Service Dependencies

The model of web service dependencies presented here is a simplification of the notion of dependency graph proposed in [4]. A dependency graph provides input / output information of available web services. Consider a web service that takes as input the ISBN number of a book and gives as output the publishing year. This information can be easily encoded using a directed graph, where the nodes, say x and y, represent ISBN number of a book and the publishing year respectively; the edge from x to y is labeled by the web service. Such a graph is called a dependency graph since the output (y) depends on the input (x), and the edge from x to y is called a dependency edge. The label may also contain information on the number of inputs and outputs. There are other types of edges called generalization or specification edges and composition/decomposition edges. These edges are used to represent the supertype-subtype relations and composite types respectively.

We make the following assumptions for dependency graphs. First, there is only one type of edge called the dependency edge. The label of an edge is simply the name of an web service. In the following we demonstrate some benefits obtained by making such assumptions.

Formally, a dependency graph G (V, E), where V is a set of nodes which represents the set of input/output of all the atomic services, E is a set of all the atomic services.

We represent a single web service as shown in Fig. 1. ***I*** is the input provided to the web service ***WS1*** and ***O*** is the output produced. ***WS1*** is the identifier of web service (like name or unique id of web service).

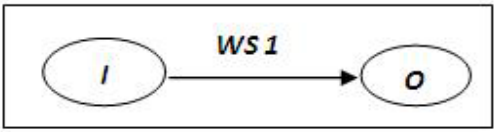


Fig. 1. A Simple Web Service Representation

We use this model of dependency graph to find composite web services. The composite web service generation process can be broadly divided into three main steps. These are as follows:

1. Extracting specification of web services
2. Relating web service specification into a dependency graph
3. Search the dependency graph for a composite service using a heuristic

The first two steps are given in the following two subsections (2.1 and 2.2). The third step is discussed in section 3.

2.1 Extracting Web Service Specification

To generate a composite service, the first requirement is to extract the web service specification from the web service description files. For extracting these specifications, web service specification languages are used. A web service specification contains the information about the type of input and output parameters accepted by the web service, the behavior of web service on conditional inputs along with the details about how to invoke the web service.

There are several web service specification languages available. We use OWL-S (Ontological Web Language for Services) as the specification language. In OWL-S each web service is specified in three XML-based parts:

(i) Service Profile**,** which includes general information about the web service, such as the name, description, inputs, and outputs.
(ii) Service Model which using structures such as sequences, conditional statements, loops, and parallel constructs show how the web service performs its functionality.
(iii) Service Grounding which contains information on how the web service can be used in practice.

We need only information from Service Profile and Service Model constructs of OWL-S for our composition purpose.

2.2 Dependency Graph Construction

We maintain a local repository containing the web service specification required for dependency graph construction. From OWL-S specifications of the web services, we store set of inputs-outputs and the dependencies information between different web services in the form of an adjacency matrix, which represents a dependency graph.

Let us consider the web service given in [4] that computes the distance between two cities. So the input to the web service WS is two cities x and y and the output is the distance d between the cities in kilometers. If we are to represent it in our dependency graph model it will have 3 nodes (x, y, d) with edges x → d and y → d. The edges are marked WS. The implicit understanding is that for WS to be meaningful, there should be exactly two inputs x and y. So the representation does not really capture the intended meaning.

Thus we perform the following operation called 'merge'. The two nodes x and y are merged to form one node labeled {x,y}. So now we have two nodes {x,y} and d and the edge <{x,y} → d > labeled WS.

In general, when there are more than one input, say x1,x2,..xk, the operation merge combines it to form one node {x1,x2,…xk}.

Suppose that there is another service WS1 that takes as input a city x and gives as output the state or county c to which it belongs. So in the dependency graph with WS and WS1, we have two nodes where x appear as a label; one for < x → c > labeled by WS1 and the other for < {x,y} → d > labeled by WS. The merge operation depends linearly on the total number of input/outputs. After the merge operation is completed the resultant dependency graph is fed as input to our search algorithm, given in the following section.

In this paper we consider web services with one output only.

3 Search Technique

In this section we develop a bidirectional heuristic search algorithm for obtaining a composite service based on the ideas presented in [7]. We propose a heuristic to facilitate the search process.

The algorithm given in [7] is a bidirectional front to front search algorithm. There are two fronts (or fringes)—one going from start to goal and the other from goal to the start node. The objective is to find a shortest path from start to goal node, if any. The algorithm is supposed to work on a state transition system where it is equally possible to work from start to goal as the other way around. The heuristic function for a node n in, say, front 1, depends on the sum of two costs: (i) the estimate of the minimum distance between nodes n and y (a node in front 2), and (ii) the cost of going from goal node to y. The idea is to select a node y from the set of nodes in front 2, such that h (n) is minimum.

Our algorithm differs from their algorithm [7] in the following ways. First, in a dependency graph it may not be always possible to work from start to goal and vice-versa. Second, for web services composition problem, we are usually looking for a composite service (a path in the dependency graph). A shortest path may not be so

meaningful in this context. Thus although the search strategy of our algorithm is like that in [5], it is more simpler and the heuristic function considered need not use estimates of minimum distance.

Proposed Heuristic

We define the heuristic value for a node *n* to be the number of nodes that are direct successors of *n*.

$$h(n) = \text{number of direct successors of node } n$$

We know that the *Index_List* set is finite and hence its size. Therefore, the heuristic is admissible. We define the heuristic to be the number of direct successors of node *n*, because as more nodes from the *Index_List* are approached, more are the chances of getting the goal node.

3.1 A Unidirectional Heuristic Search Algorithm (HS)

We use the terminology given in [7].

s: start node, *g*: goal node
S: collection of nodes reached from s which were expanded
S': collection of nodes which are not in S but are direct successor of nodes in S
h(n): heuristic value for node *n*, $n \in$ S'
Index_List: set of intersection of inputs and outputs of all web services.

The search algorithm is given below:

1. S = *get_outgoing_node_list(s)* /* get all the successor of *s* and place in S */
2. S' = *get_outgoing_node_list(*S*)* /* get all the successors of nodes in S */
3. **if** g $\in$ (S $\cup$ S') **then** success and stop
4. otherwise, **if** (|S| + |S'|) $\geq$ | *Index_List* | **then** stop and report failure
5. **else**
   (i) get the node, say *x*, from S' such that *h(x)* is maximum
   (ii) remove *x* from S' and add it to S
   (iii) S' $\leftarrow$ S' $\cup$ (successors of *x*)
   (iv) **if** g $\in$ S' **then** return the path from s to g **else** GOTO step 4

The above algorithm works fine in most of the cases and the time taken to search is less than the execution time of Breadth First Search (BFS), Depth First Search (DFS) and Bidirectional Breadth First Search algorithm (BdBFS). But for some cases it gets stuck and takes much more time than BFS, DFS and BdBFS. One such case is listed in Fig. 2.

The node X in Fig. 2 will be expanded after most of the nodes at the second last level are expanded, hence it will take significant time to reach node X with our heuristic. The node X is not expanded by the heuristic search in the beginning irrespective of the fact that node X's parent is adjacent to a node in S'. This is because h(Y) = 1 where Y is the parent of X. So, the time taken to reach X using our heuristic is, in general, more than the time taken by other algorithms.

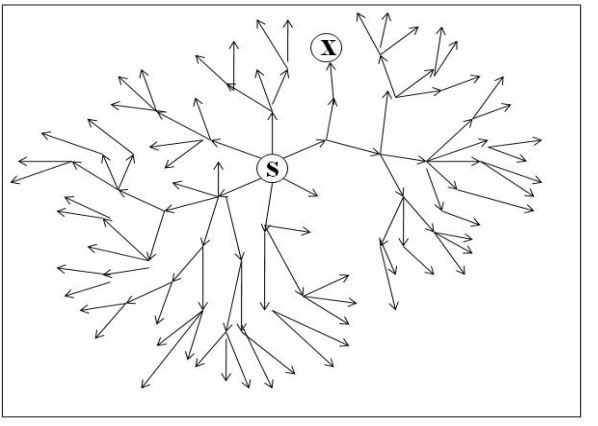


Fig. 2. An instance showing the problem with the above algorithmS represents here the start node

To overcome this limitation, we suggest that the notion of ageing be included in the nodes. We increment the age of a node from the moment the node is added to S' to the moment it is being removed from S' and placed in S. So, the age of a node is initialized in line 2 and its value is incremented in line 5 (iii). We have chosen a threshold for *age_limit*. Any node in S' whose age is more than the *age_limit* is returned irrespective of its *h (n)* value. From the several experiments that we conducted, we found that using

$$age\_limit = 0.1 * |Index\_List|$$

best execution time is achieved. For *age_limit* = 1 the algorithm works as the standard bidirectional breadth first search algorithm.

Using the notion of ageing, the node X in Fig. 2 would be picked up after some number of steps, as obtained by the *age_limit.* If this was not considered then the node X might have starved for a much longer time for it to be picked up. This criterion plays a significant role especially when the size of the dependency graph is large.

We are now set to present a bidirectional search technique that uses the heuristic defined above.

3.2 A Bidirectional Heuristic Search Algorithm (BdHS)

Terminology:

s: start node
g: goal node
S: collection of nodes reached from s which were expanded
S': collection of nodes which are not in S but are direct successor of nodes in S
h1 (n): heuristic value for node *n*, $n \in$ S'
G: collection of nodes reached from g which were expanded (here we reverse the direction of the edges during traversal)

G': collection of nodes which are not in G but are direct successor of nodes in G
h2 (n): heuristic value for node *n*, $n \in$ G'.
Index_List: set of intersection of inputs and outputs of all web services.

The bidirectional heuristic search algorithm proceeds as follows:

1. S = *get_outgoing_node_list(s)* /* get all the successor of *s* and place in S */
2. S' = *get_outgoing_node_list*(S) /* get all the successors of nodes in S */
3. **if** g $\in$ (S $\cup$ S') **then** success and stop
4. G = *get_outgoing_node_list(g)* /* get all the successor of *g* and place in G */
5. G' = *get_outgoing_node_list(G)* /* get all the successors of nodes in G */
6. **if** S' $\cap$ G' $\neq \varnothing$ **then** return path from start node *s* to goal node *g*
7. otherwise, **if** (|S| + |S' | + |G| + |G'|) $\geq$ | *Index_List* | **then** stop report failure
8. **else**
   i. get the node, say *x*, from S' such that *h1(x)* is maximum
   ii. remove *x* from S' and add it to S
   iii. S' $\leftarrow$ S' $\cup$ (successors of *x*)
   iv. get the node, say *y*, from G' such that *h2(y)* is maximum
   v. remove *y* from G' and add it to G
   vi. G' $\leftarrow$ G' $\cup$ (successors of *y*)
   vii. **if** g $\in$ (S' $\cup$ G') **then** return the path from s to g **else** GOTO step 7

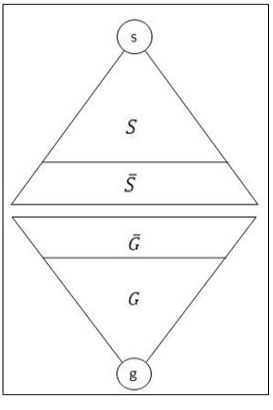


Fig. 3. Search propagation for the Bidirectional Heuristic Search Algorithm

The algorithm BdHS closely resembles the algorithm HS given in section 3.1. The search propagation for BdHS is shown in Fig. 3. BdHS can be viewed as an extension of HS in the sense that the search now proceeds in both directions; one going from the start node s to goal node g and other in the opposite direction. In order to accommodate the bidirectional search, we have included the sets G, G', the heuristics h1, h2, and the corresponding conditions in lines 7 and 8.

Our algorithm is best suitable for dense graphs, because the heuristic expands the densest regions of the graph. After including ageing technique, the execution of the algorithm gives efficient and fast results. The results of the execution are discussed in the next section.

4 Experimental Results

We have implemented the dependency graph construction algorithm and the bidirectional heuristic search algorithm in JAVA using NetBeans IDE 6.1. All the executions are done on a personal computer having the following specifications: T500 Intel Core 2 CPU Processor, clock frequency 1.60 GHz, and 2 GB RAM.

4.1 Execution of Dependency Graph Construction Algorithm

Table 1 shows the results of executing dependency graph construction algorithm on 4 different sets of web services. The web service count represents the number of atomic web services generated. Nodes count represents the number of different inputs and outputs involved in the set of available web services.

Table 1. Execution Time for Dependency Graph Construction

S. No	Number of nodes / number of atomic web services	Average Execution Time (in milliseconds)
1	Nodes: 11, Web Services: 15	160.2
2	Nodes: 50, Web Services: 67	2622.4
3	Nodes: 100, Web Services: 187	10985.5
4	Nodes: 200, Web Services: 332	22885.5

4.2 Execution of Bidirectional Heuristic Search Algorithm

We present the results of executing different graph search algorithms and our algorithms on the four dependency graphs given in the previous subsection (4.1). These algorithms include: Breadth First Search (BFS), Depth First Search (DFS), Bidirectional Breadth First Search (BdBFS), Heuristic Search (HS), and Bidirectional Heuristic Search (BdHS).

Fig. 4 shows a simple dependency graph with nodes representing inputs accepted and outputs produced by web services. The labels of the directed edges in the figure represent the web services involved. For simplicity we have named the nodes with alphabets (A, B, C,..) and the web services with numbers (1, 2, 3,…).

In Fig. 5 the chart shows the execution time of the different algorithms for the dependency graph considered in Fig. 4 and the queries given in Table 2. The results reflect that the execution times for all the algorithms are nearly the same. This is so since the size of the graph considered is quite small.

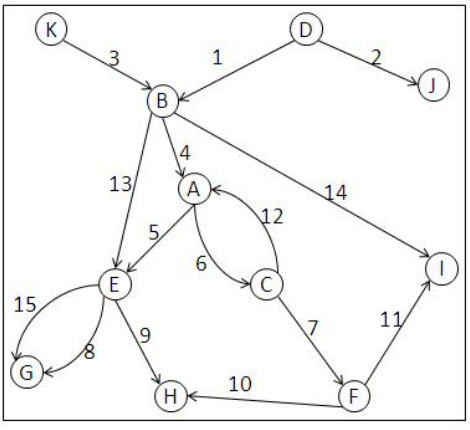


Fig. 4. A Dependency Graph1 with 11 nodes and 15 web services

Table 2. Paths found by the Search Algorithms for Different Queries

Dependency	Path	Execution of web services
B→ F	B^4→ A^6 → C^7→ F	Executing web service 4,6,7 in order
K→ E	K^3→ B^{13} → E	Executing web service 3,13 in order
C→ I	C^7→ F^{11} → I	Executing web service 7,11 in order
B→ H	B^{13}→ E^9 → H	Executing web service 13,9 in order

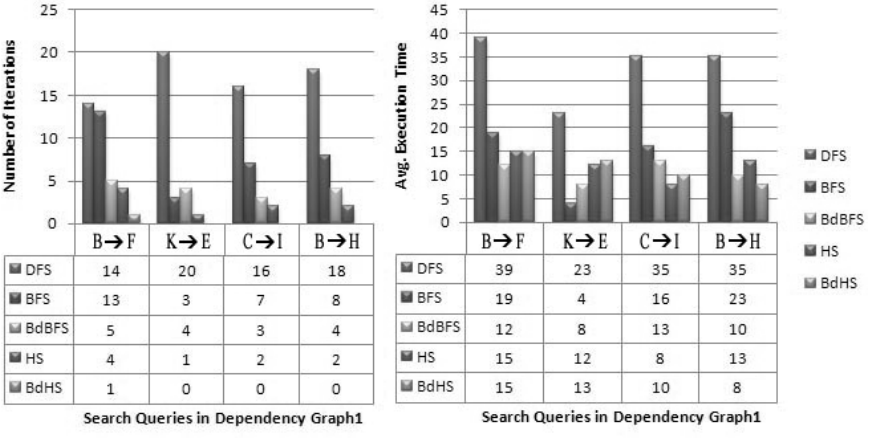
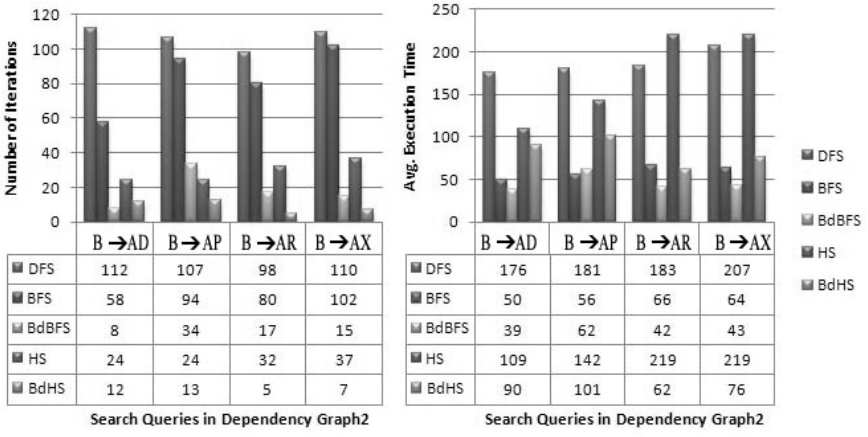


Fig. 5. Results of executing different algorithms for the four different queries on Dependency Graph1. Execution time is in milliseconds.



	B →AD	B →AP	B →AR	B →AX
DFS	112	107	98	110
BFS	58	94	80	102
BdBFS	8	34	17	15
HS	24	24	32	37
BdHS	12	13	5	7

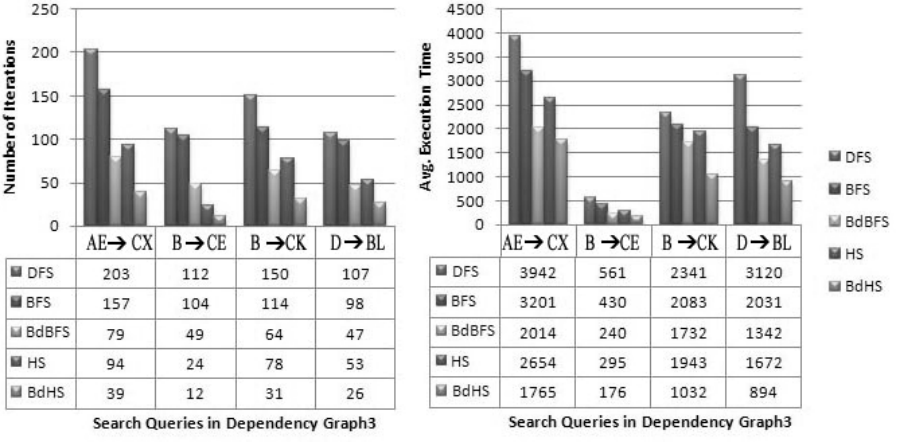
	B →AD	B →AP	B →AR	B →AX
DFS	176	181	183	207
BFS	50	56	66	64
BdBFS	39	62	42	43
HS	109	142	219	219
BdHS	90	101	62	76

Fig. 6. Results of executing different algorithms for the four different queries on Dependency Graph 2. Execution time is in milliseconds.

Now we test the five algorithms on a larger dependency graph (Dependency Graph2 having 50 nodes and 67 web services) .We have named the nodes with simple strings and the web services as numbers. Dependency Graph2 contains nodes, namely A-Z and AA-AX, and web services numbered from 1-67. The results are shown in Fig. 6.

In the following figures (Fig. 7 and Fig. 8) we give the results showing the execution time of different algorithms on large sized dependency graphs.

Dependency Graph3 contains 100 nodes (A-Z, AA-AZ, BA-BZ) and CA-CV and 187 web services numbered 1-187. Dependency Graph4 contains 200 nodes (A-Z, AA-AZ, BA-BZ, CA-CZ, DA-DZ, EA-EZ, FA-FZ and GA-GH) and 332 web services numbered 1-332.



	AE→ CX	B →CE	B →CK	D→BL
DFS	203	112	150	107
BFS	157	104	114	98
BdBFS	79	49	64	47
HS	94	24	78	53
BdHS	39	12	31	26

	AE→ CX	B →CE	B →CK	D→BL
DFS	3942	561	2341	3120
BFS	3201	430	2083	2031
BdBFS	2014	240	1732	1342
HS	2654	295	1943	1672
BdHS	1765	176	1032	894

Fig. 7. Results of executing different algorithms for the four different queries on Dependency Graph3. Execution time is in milliseconds.

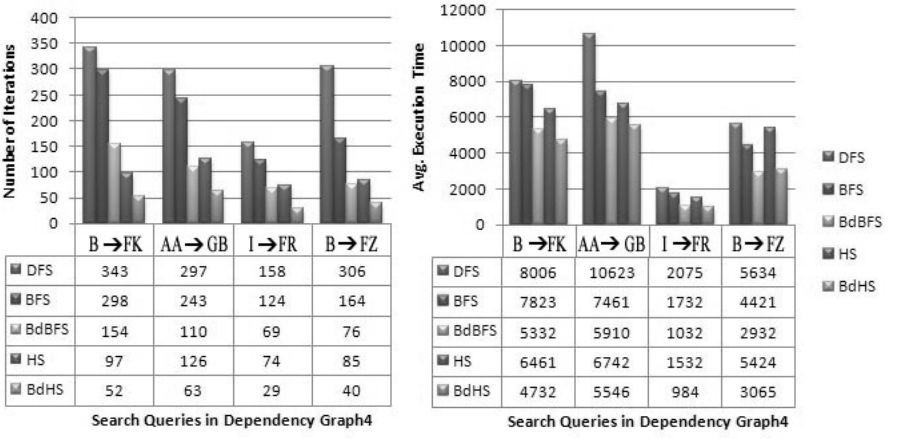


Fig. 8. Results of executing different algorithms for the four different queries on Dependency Graph4. Execution time is in milliseconds.

We have executed the algorithm only for those inputs and outputs for which the path to be traversed is large. This is to show the difference in the average time taken by different methods to search for a composite service.

The results in Figures 5 and 6 shows that the difference in execution time and number of iterations of bidirectional heuristic algorithm and other algorithms is not significant. However, the results in Figures 7 and 8 show a significant difference in execution time and number of iterations of the bidirectional heuristic algorithm and other algorithms. We can see that as the number of nodes and number of web services involved increases, the efficiency of our algorithm also increases. Thus for large graphs our algorithm can prove very efficient in terms of computational time and performance.

5 Discussion

In this paper we adopted the notion of dependency graph introduced in [4,5] to model web services. Some features of the dependency graph [4] were considered. For this dependency graph we developed a search algorithm to construct to a composite web service. The search algorithm is based on the ideas of an existing algorithm [7]. We defined a new domain independent heuristic and the results demonstrate its advantages over some of the well known search algorithms.

Most of the implemented systems for web services composition are based on AI planning. Some of these systems are developed in [8] [9]. However, we are not aware of any heuristic search algorithms used for web services composition.

A working system that fully implements the web service composition algorithm given in [4] may prove to be useful. That is, we now have a composite web service for a dependency graph with all the three types of edges [4]. It may be observed that the complexity of such a system would be much more than the one developed in this paper.

We would like to implement it as part of our future work. Another direction of our ongoing/future work would be to define a suitable heuristic for a specific application. This may lead to a substantial improvement in the performance.

It would be quite interesting to study the difficulty of adapting our composition scheme for other domains that require general services/resources composition, such as retrieval engines, automatic translators, business services, and social networks.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable suggestions.

References

1. Dustdar, S., Schreiner, W.: A survey on web services composition. Int. Journal on Web and Grid Services 1(1), 1–30 (2005)
2. Rao, J., Su, X.: A survey of automated web services composition methods. In: Cardoso, J., Sheth, A.P. (eds.) SWSWPC 2004. LNCS, vol. 3387, pp. 43–54. Springer, Heidelberg (2005)
3. Milani, A., Rossi, F., Pallottelli, S.: Planning Based Integration of Web Services. In: Proceedings of the IEEE/WIC/ACM Int. Conf. on Web intelligence and Intelligent Agent Technology, Washington, DC, pp. 125–128 (2006)
4. Hashemian, S.V., Mavaddat, F.: A Graph-Based Framework for Composition of Stateless Web Services. In: Proceedings of the European Conference on Web Services, pp. 75–86 (2006)
5. Hashemian, S.V., Mavaddat, F.: A graph-based approach to web services composition. In: Proceedings of the 2005 Symposium on Applications and the Internet (SAINT), pp. 183–189 (2005)
6. Ashish, N., Knoblock, C.A.: Wrapper generation for semi-structured Internet sources. SIGMOD Record 26(2), 8–15 (1997)
7. Champeaux, D., Sint, L.: An improved bidirectional heuristic search algorithm. JACM 24(2), 177–191 (1977)
8. Ponnekanti, S.R., Fox, A.: SWORD: A developer toolkit for web service composition. In: Proceedings of 11th world wide web conference, USA (2002)
9. Wu, D., Sirin, E., Hendler, J., Nau, D., Parsia, B.: Automatic web services composition using SHOP2. In: Workshop on Planning for Web Services, Italy (2003)

Evolutionary Optimized Networks for Consensus and Synchronization

Toshihiko Yamamoto and Akira Namatame

Department of Computer Science, National Defense Academy of Japan,
Yokosuka, Hashirimizu 1-10-20, Japan
{g47038,nama}@nda.ac.jp

Abstract. Collective behavior in nature, the interaction between agents and factors, there is consensus problem as an important characteristic for coordinated control problem. Consensus problem is closely related to the complex networks. Recently, many studies are being considered in the complex network structure, the question what network is the most suitable to the property of the purpose has not been answered yet in many areas. In the previous study, network model has been created under the regular rules, and investigated their characteristics. But in this study, network is evolved to suit the characteristics of the objection by evolutionary algorithm and we create optimized network. As a function of the adaptive optimization, we consider the objection that combinate consensus, synchronization index and the density of the link, and create the optimized network which is suitable to the property of the objective function by evolutionary algorithms. Optimal networks that we design have better synchronization and consensus property in terms of the convergence speed and network eigenvalues. We show that the convergence speed is faster in evolutionary optimized networks than previous networks which are known as better synchronization networks. As a result, we generate optimal consensus and synchronous network.

Keywords: Evolutionary Optimization, Genetic Algorithm, Consensus, Synchronization, Complex networks.

1 Introduction

Synchronization and collective behavior phenomena such as herd behavior and cries in nature [1] [2] and human society consensus of opinion, the problem of coordinated control of agents robots [3] [4] [5] are being treated as important issues by the interaction between elements of emergent phenomena. And the problem can be viewed as a consensus problem. It is closely related to the properties of complex networks. Recently, many studies are being considered in the complex network structure, the question what network is the most suitable to the property of the purpose has not been answered yet in many areas. Many essential features displayed by complex systems emerge from their underlying network structure [6] [7]. Different mechanisms have been suggested to explain the emergence of

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 321–335, 2010.

the striking features displayed by complex networks. When dealing with biological networks, the interplay between emergent properties derived from network growth and selection pressures has to be taken into account. As an example, metabolic networks seem to result from an evolutionary history in which both preferential attachment and optimization are present. This view corresponds to Kauffman's suggestion that evolution would operate by taking advantage of some robust, generic mechanisms of structure formation [7]. Synchronous behavior is also affected by the network structure. The range of stability of a synchronized state is a measure of the system ability to yield a coherent response and to distribute information efficiently among its elements, while a loss of stability fosters pattern formation [8].

In the previous study, network model has been created under the regular rules, and investigated their characteristics. As prominent examples, random network [9], small-world network [10], scale free network [11] are raised. And there are many other network models based on local making rule. But in this study, network is evolved to suit the characteristics of the objection by evolutionary algorithm and we create optimized network. As a function of the adaptive optimization, we consider the objection that combinate consensus, synchronization index and the density of the link, and create the optimized network which is suitable to the property of the objective function by evolutionary algorithms. Optimal networks that we design have better synchronization and consensus property in terms of the convergence speed and network eigenvalues. We show that the convergence speed is faster in evolutionary optimized networks than previous networks which are known as better synchronization networks. As a result, we generate optimal consensus and synchronous network.

2 Consensus Problems and Synchronization

Consensus problems have a long history in computer science and control theory [4]. In networks of agents, consensus means to reach an agreement regarding a certain quantity of interest that depends on the state of all agents. A consensus algorithm is an interaction rule that specifies the information exchange between an agent and all of its neighbors on the network. The theoretical framework for solving consensus problems for networked systems was introduced by Olfati-Saber and colleagues [3].

The analysis of consensus problems relies heavily on matrix theory and spectral graph theory. The interaction topology of a network of agents is represented using a directed graph G with the set of nodes and edges. We denote neighbors of agent i with n_i.

Consider a network of agents with the following dynamics:

$$\dot{x}_i = \sum_{j \in N_i} \alpha_{ij} \left(x_j(t) - x_i(t) \right) \tag{1}$$

where a_{ij} is the weight of agent i on agent j. Here, reaching a consensus means asymptotically converging to the same internal state by way of an agreement characterized by the following equation:

$$x_1 = x_2 = \cdots = x_n = \alpha \tag{2}$$

Assuming that the underlying graph G is undirected ($a_{ij} = a_{ji}$ for all i, j), the collective dynamics converge to the average of the initial states of all agents:

$$\alpha = \frac{1}{n} \sum_{i=1}^{n} x_i(0) \tag{3}$$

The dynamics of system in Eq. 1 can be expressed as

$$\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}(t) \tag{4}$$

$\mathbf{L}$ is the graph Laplacian of the network G; the graph Laplacian is defined as

$$\mathbf{L} = D - A \tag{5}$$

where $D = \text{diag}(d_1, d_2, \cdots, d_n)$ is the diagonal matrix with elements $d_i = \sum_{j \neq i} a_{ij}$ and A is the binary adjacency matrix ($n \times n$ matrix) with elements a_{ij} for all i, j where is 1 if agent i and agent j is connected or 0 if they are disconnected.

Notice that because our networks are undirected, L is a symmetric matrix with all real entries, and therefore a Hermitian matrix. In our case this is always met with equality, since the diagonal entry of each row in L is the degree of node i, and each link connected to i results in -1 in the same row. So the sum of all off diagonals in a row is a_{ii}. Therefore L is a positive semi-definite matrix. Since L is semi-definite (and therefore also Hermitian), we will adopt the ordering convention

$$0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n \tag{6}$$

We can also ask how synchronizability depend upon network topology does in the same framework. An answer to this question was given in a seminal work by Barahona and Pecora who established the following criterion to determine the stability of fully synchronized states on networks [8] [12]. Consider a general dynamical process

$$\dot{x}_i = F(x_i) - \sigma \sum_j L_{ij} H(X_i) \tag{7}$$

where x_i with $i \in 1, 2, \ldots, n$ are dynamical variables, F and H are an evolution and a coupling function respectively, and σ is a constant. A standard linear stability analysis can be performed by i) expanding around a fully synchronized state

$$x_1 = x_2 = \cdots = x_n = x^s \tag{8}$$

with x^s solution of $\dot{x}^s = F(x^s)$, ii) diagonalizing L to find its n eigenvalues, and iii) writing equations for the normal modes y_i of perturbations

$$\dot{y}_i = \left[F'(x^S) - \sigma\lambda_i H'(x^s)\right] y_i \tag{9}$$

all of them with the same form but different effective couplings $\alpha = \sigma\lambda_i$. Barahona and Pecora noticed that the maximum Lyapunov exponent for Eq. 9 is, in general, negative only within a bounded interval $[\alpha_A, \alpha_B]$, and that it is a decreasing (increasing) function below (above). Requiring all effective couplings to lie within such an interval,

$$\alpha_A < \sigma\lambda_2 \leq \ldots \leq \sigma\lambda_n < \alpha_B \tag{10}$$

one concludes that a synchronized state is linearly stable if and only if $\frac{\lambda_n}{\lambda_2} < \frac{\alpha_B}{\alpha_A}$ for the corresponding network. It is remarkable that the left hand side depends only on the network topology while the right hand side depends exclusively on the dynamics (through F and G, and x_s).

Therefore, the interval in which the synchronized state is stable is larger for a smaller ratio of the two eigenvalues λ_n/λ_2, and a network has a more robust synchronized state if the ratio

$$Q = \frac{\lambda_n}{\lambda_2} \tag{11}$$

which is also known as algebraic connectivity, is as small as possible [4].

Also, as the range of variability of λ_n is limited (it is related to the maximum connectivity) minimizing Q gives very similar results to maximizing the denominator λ_2 in most cases. Especially, λ_n expresses robustness to delays i.e. if λ_n is small, the network has good consensus. Indeed, as argued in [13], in cases where the maximum Lyapunov exponent is negative in an un-bounded from above interval, the best synchronizability is obtained by maximizing the algebraic connectivity.

3 Definition of Objective Functions

In this simulation, we define that the objective function include both eigenvalue ratio and link cost. Thus, we will optimize networks through eigenvalue ratio and link cost on same time.

3.1 Eigenvalue Ratio

We want to optimize a network what have minimum eigenvalue ratio, so Eq. 11 is set to object function. We can optimize a network through selection of minimize network. So, we optimize a network both maximization of λ_2 and minimization λ_n that is, we obtain a network with the minimum the λ_n/λ_2 algebraic connectivity.

3.2 Average Degree

Many essential features of links are displayed by complex systems: for example, memory, stability and homeostasis emerge from the underlying network structure [6]. Different networks exhibit different features at different levels, but most complex networks are extremely sparse and exhibit the so-called small-world phenomenon [10].

We can predict that the network of minimum eigenvalue ratio is complete network (Thus $\lambda_n/\lambda_2 \geq 1$). Therefore, we add eigenvalue ratio to Average degree. And, average degree is defined

$$\langle k \rangle = \frac{2}{n} \sum_{k=1}^{n} a_{ij} \tag{12}$$

3.3 Weighted Object Function

In this simulation, the evaluation function of our optimization algorithm is optimization of both Eq. 11 and Eq. 12 at the same time.

In this simulation, we will optimize networks through importance of link constraint.

There is a large gap between eigenvalue ratio λ_n/λ_2 and average degree $\langle k \rangle$. And, in this case, we use any constant for balance. Because, optimized networks are much alike in characteristic i.e. there is not important.

Therefore, the object function optimized for consensus and synchronization is defined as

$$E(\omega) = \omega \frac{1}{\lambda_2} + (1 - \omega) \langle k \rangle \tag{13}$$

$$E(\omega) = \omega \left(\frac{\lambda_n}{\lambda_2} \right) + (1 - \omega) \langle k \rangle \tag{14}$$

where ω $(0 \leq \omega \leq 1)$ is a parameter controlling objects $1/\lambda_2$, λ_n/λ_2 and $\langle k \rangle$. We know that $\omega = 0$ is the minimization problem for just average degree $\langle k \rangle$ and $\omega = 1$ is the minimization problem for just eigenvalue $1/\lambda_2$, λ_n/λ_2.

4 The Evolutionary Optimization Method

Initially we prepare 50 undirected graphs, each graph has a fixed number of nodes n and links defined by the binary adjacency matrix $A = [a_{ij}]$, $1 \leq i, j \leq n$. The adjacency matrix A is $n \times n$ matrix because of award for all nodes and a symmetry matrix because of an undirected graph.

4.1 Initial Networks

Initially 50 networks were generated by a specified probability about links. number per node is 7, and the degree distribution obeys a Poisson distribution. In

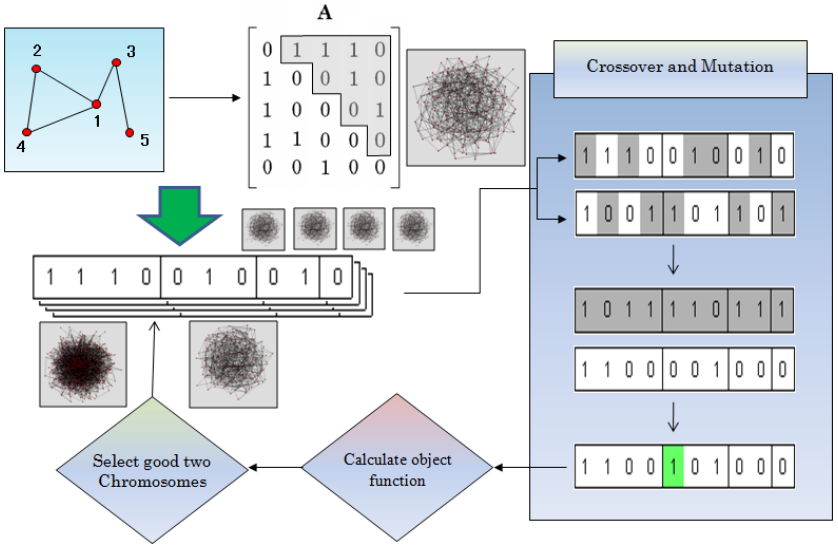


Fig. 1. The basic scheme of the genetic algorithm for optimizing networks

other words, an initially designed network is a random network. We generate ten random networks that resemble this and we use the genetic algorithm to obtain better networks in terms of improving the fitness function in (13),(14).

4.2 Genetic Algorithm

In this study, the system uses the genetic algorithm to generate an optimized network structure. Especially we use the MGG model for the change of generations [14]. Especially we select two best networks and their adjacency matrices are crossover as shown in Figure 1 in order to generate two better networks.

We use crossover rate at 0.7, and mutation rate is set at $2/{}_nC_2$, i.e. reverses of two links per one generation. We create 50 different networks as individuals at the beginning. And, we stop until the object function has almost the same value match on ${}_nC_2$ generations.

The model uses an encoded network by the binary adjacency matrix for the mutation and crossover. Next, the most suitable matrices among the parents and children matrices are chosen, and the others are eliminated.

We used the multi-point crossover. After crossover, each element in the matrix switches to a reverse state with a specific probability. In this paper, the network is an undirected graph, and so, if one element is reversed, the symmetry element is reversed at the same time.

There is the possibility that an isolated network appears after crossover and mutation. In this paper, when an isolated node appears in a new network that the node has 0 distances to another node, we dump the network. Therefore, we can use non-isolated matrices. After long generations have passed, we can obtain an optimal network which minimizes the fitness function defined in (13),(14).

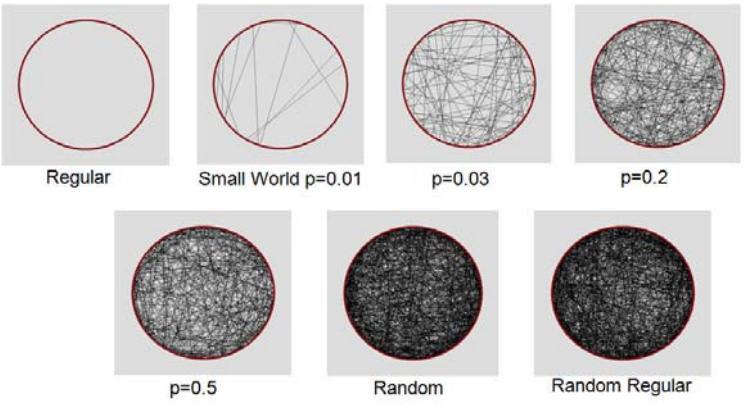


Fig. 2. Previous network models we compare(regular network, random network, small-world network and random regular network)

5 Optimized Networks Generated

5.1 Previous Conventional Network Models

On the network consensus and synchronization problem, That Laplacian matrix 2nd smallest eigenvalue is high means the algebraic connectivity of the network is high, and the network have the characteristics of fast convergence to the solution of the consensus and synchronization problem. Previous conventional network models which are valid for consensus and synchronization problem are small-world networks [10]. In previous studies, small-world networks' the convergence speed is faster and more effective than regular network [15] [4].

Regular network models have the same degree connected to neighborhood nodes, such network model of λ_2 is low, so convergence speed is slow. But small-world networks are randomly chosen nodes and rewired by link probability $0 \leq p \leq 1$, so λ_2 have higher value. In the case of probability $p = 0$, the network is regular network, and when probability is $p = 1$ the network is random network [9]. Random network and small-world networks whose p is close to $p = 1$ have high algebraic connectivity property, therefore the networks show fast convergence and good consensus and synchronization property.

Furthermore, random regular(or Ramanujan graph) network is the network model which have higher algebraic connectivity rather than random network and small-world networks [16] [17] [18]. Random regular network have the same degree as regular network. Regular network have the same degree connected to neighborhood nodes, but random regular network have links that stretched to other nodes randomly. Random regular network have high homogeneous property and larger algebraic connectivity because of the same degree and random links that stretched to other nodes. Therefore, Random network and small-world networks whose p is close to $p = 1$ have high algebraic connectivity property, but random regular network have larger algebraic connectivity than random network and small-world networks.

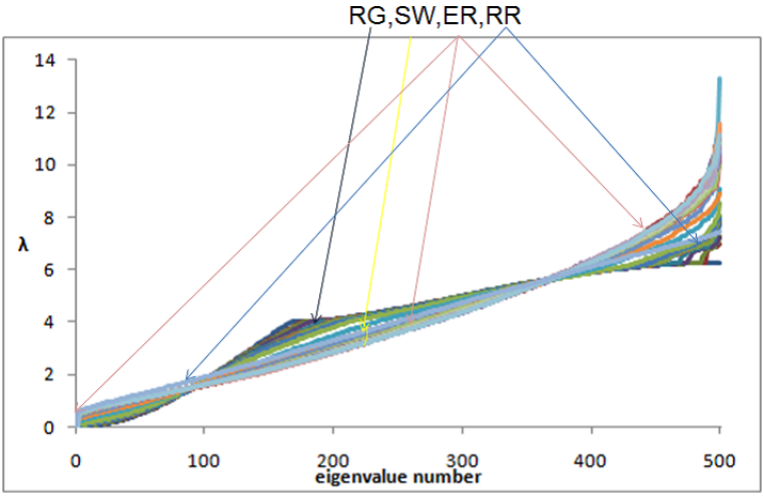


Fig. 3. All Laplacian eigenvalue transition of the previous network models

These previous network models(regular network, random network, small-world network and random regular network)(Figure 2) are the comparing models with our optimized networks. Figure 3 shows all Laplacian eigenvalue transition of the previous network models(regular network, random network, small-world networks and random regular network), and 2nd Laplacian eigenvalue of the previous network models are shown in Figure 4 to compare algebraic connectivity. In figure, RG,SW,ER,RR represents regular network, small-world networks, random network, random regular network respectively. Number of nodes is 500, so the number of all eigenvalues are 500.

From Figure 4 regular network is low algebraic connectivity, and small-world networks' algebraic connectivity are becoming higer as p is increasing. Random

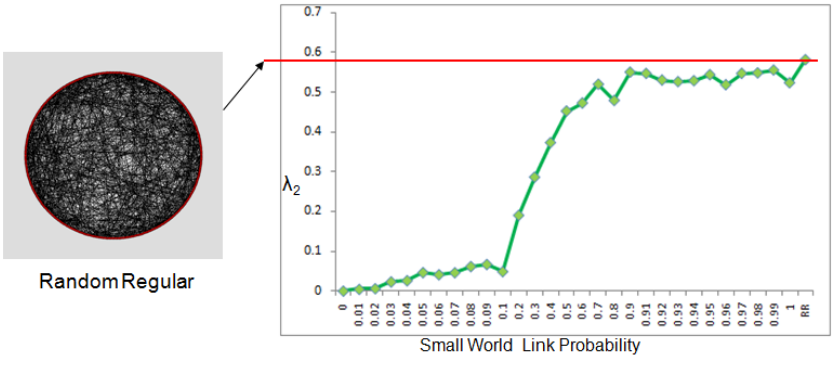


Fig. 4. 2nd smallest Laplacian eigenvalues of the previous network models

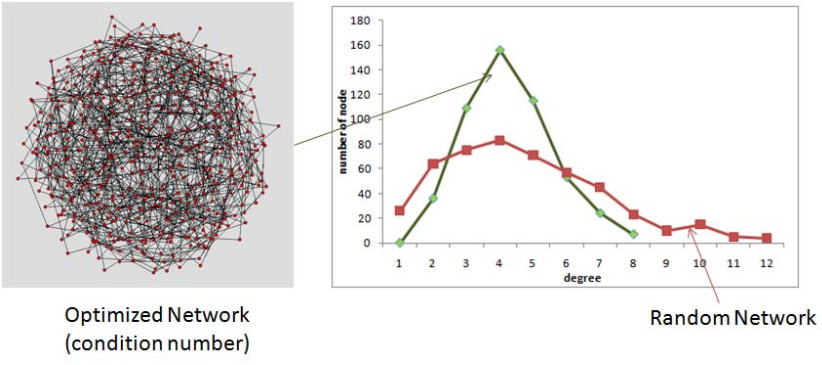


Fig. 5. Optimized networks(condition number) and degree distribution

network and small-world networks whose p is close to $p = 1$ have high algebraic connectivity property of all network based on link probablity p, and random regular network have larger algebraic connectivity than those networks.

5.2 Optimized Networks Comparison with Previous Networks

The structure of the optimal networks generated evolutionary algorithm is shown in Figure 5,6 by degree distribution. In order to examine how optimal networks are suitable and effective on the consensus and synchronization problem, We compare optimal networks with the previous network models. And the average degree is almost equivalent to assure comparing, the average degree is 4. Optimized networks are homogeneous networks having almost the same degree and node-to-node distance. However the optimized network is not random regular networks in which all nodes have the same degrees nor random networks whose degree distribution is poisson degree distribution.

In the previous network models, we can understand that random regular network is the highest algebraic connectivity. Figure 7 shows that optimized networks comparing with the previous network model by 2 smallest eigenvalue. Optimzed networks by λ_2 or by condition number have property whose algebraic connectivity is superior than the previous network models. From Figure 7 we can see that the 2nd smallest eigenvalue is much greater in evolutionary optimized networks than random regular(Ramanujan graph) networks which are the highest algebraic connectivity networks in the previous network models(regular network, random network, small-world network and random regular network).

To be considered stable conditions for consensus and synchronization robustness of information and communication by time delay and fast convergence speed, Smaller the Laplacian matrix eigenvalue ratio of 2nd smallest eigenvalue and maximum eigenvalue Q(condition number) is, the better network structure has properties for consensus and synchronization. Figure 8 shows that optimized networks comparing with the previous network model by maximum eigenvalues. And Figure 9 shows that optimized networks comparing with the previous network model by Q(condition number).

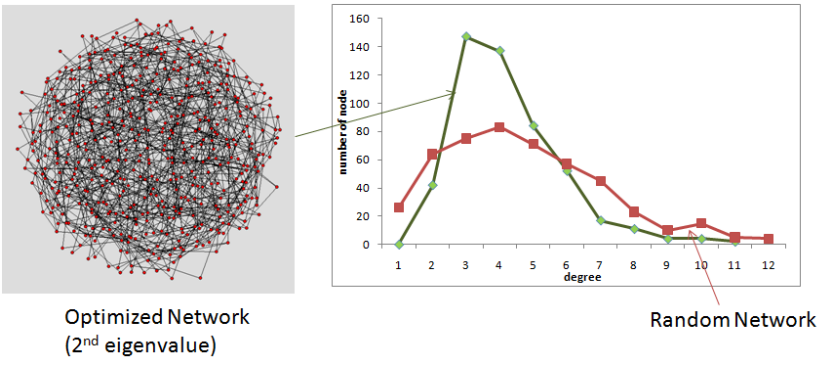


Fig. 6. Optimized networks(2nd eigenvalue) and degree distribution

As the probability rises from small-world links, the maximum eigenvalue go up high in Figure 8, which shows the characteristics of random regular network lower maximum eigenvalue. Because random regular network has similar characteristics of regular network which has same degree for all nodes. As we see in Figure 4, random regular network have larger algebraic connectivity than random network and small-world networks. Random regular network have high homogeneous property and larger algebraic connectivity because of the same degree and random links that stretched to other nodes. But, optimized networks we propose have comparatively better maximum eigenvalue property than small-world networks whose p is close to $p = 1$, and furthermore, optimized networks have far better algebraic connectivity and Q(condition number) values than random regular networks which are currently known as the best networks in the literatures and previous network models. That is why we can say that our optimized networks are better networks for consensus and synchronization in comparison to all the network models which are known.

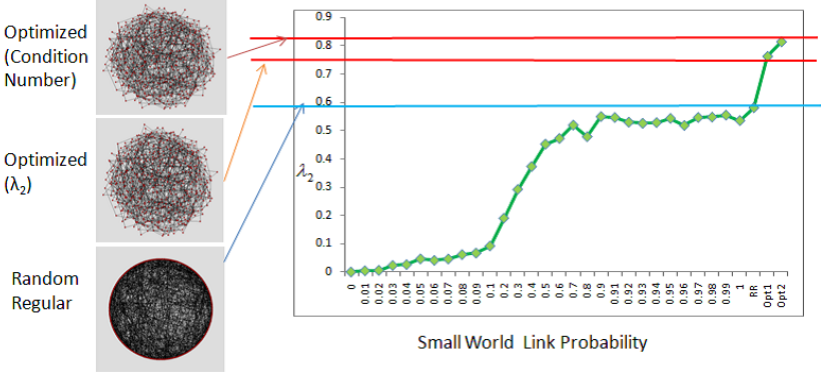


Fig. 7. 2nd smallest Laplacian eigenvalues of the optimized networks and previous network models

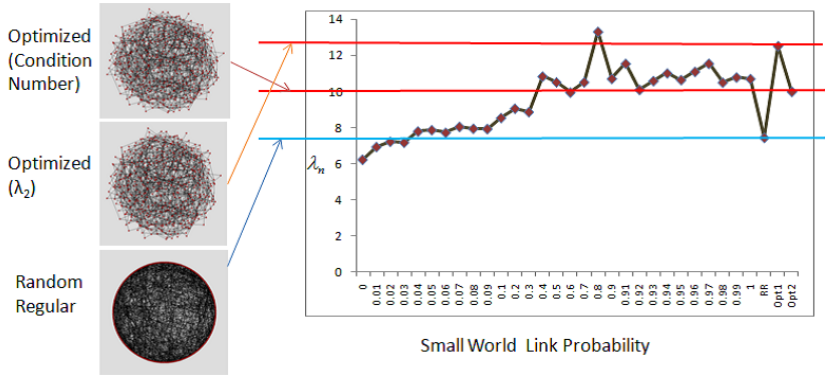


Fig. 8. Maximum Laplacian eigenvalues of the optimized networks and previous network models

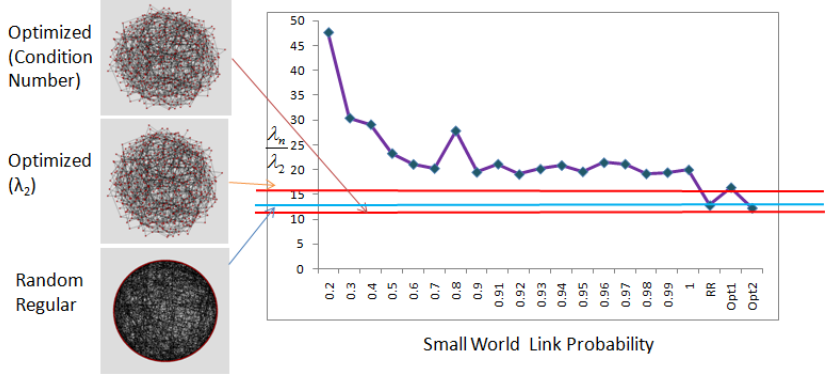


Fig. 9. Q(condition number) of the optimized networks and previous network models

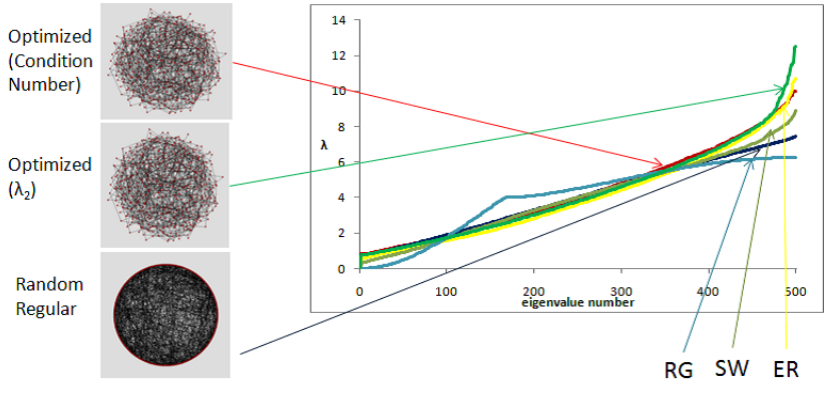


Fig. 10. All Laplacian eigenvalues transition of the representative networks

We can understand these networks properties from all Laplacian eigenvalues transition. These all eigenvalues transition of the optimized networks, regular network, random network, small-world networks($p = 0.2$ as representation of algebraic connectivity starting going up high) and random regular network are shown in Figure 10.

The 2nd smallest Laplacian eigenvalue of optimized networks is highest, and random regular network, random network, small-world networks($p = 0.2$ as representation) follow, regular network is the lowest. Eigenvalues of the Laplacian matrix of regular network is fluctuating eigenvalue transition in the middle rising, the maximum and minimum eigenvalue are relatively low. Eigenvalues of the Laplacian matrix of random network increase exponentially, small-world networks have intermediate characteristics between regular network and random network. Eigenvalues of the Laplacian matrix of random regular network increases linearly because of homogeneous property. And optimized network(optimized by λ_2) has the higher algebraic connectivity than previous network models, but maximum eigenvalue property is higher than optimized network(optimized by condition number). So optimized network(optimized by λ_2) dose not have better property for consensus and synchronization than optimized network(optimized by condition number). And optimized network(optimized by condition number) has better network property for consensus and synchronization which has the highest algebraic connectivity and comparatively lower maximum eigenvalue property than small-world networks whose p is close to $p = 1$. Because optimized network(optimized by condition number) is considered by both maximum eigenvalue and 2nd smallest eigenvalue. As a result, optimized networks have the lowest Q(condition number), and we can say optimized networks have the best property for consensus and synchronization.

5.3 Comparison of Consensus and Synchronization Convergence Speed

As we see so far, by comparing the optimal networks generated by evolutionary algorithm with the previous network models, we can understand that optimized networks have the best property for consensus and synchronization whose algebraic connectivity and Q(condition number) are better than previous network models.

To examine how fast the process of achieving consensus of the networks are, we compare convergence speed property of the networks which we see so far about the algebraic connectivity and Q(condition number) on the consensus problems.

As the following equation Eq.15, the initial various values of each nodes are given at first.

$$x_i(0) = i(i = 1, 2, \cdots, n) \tag{15}$$

And each n agents(nodes) for the system, the state of each agents x_i, $(1 \leq i < n)$ shown in chapter.2 converge to a constant value, Comparing the time required for achieving consensus. That is, until asymptotically converging to the same internal state by way of an agreement characterized by the following equation:

$$x_1 = x_2 = \cdots = x_n \tag{16}$$

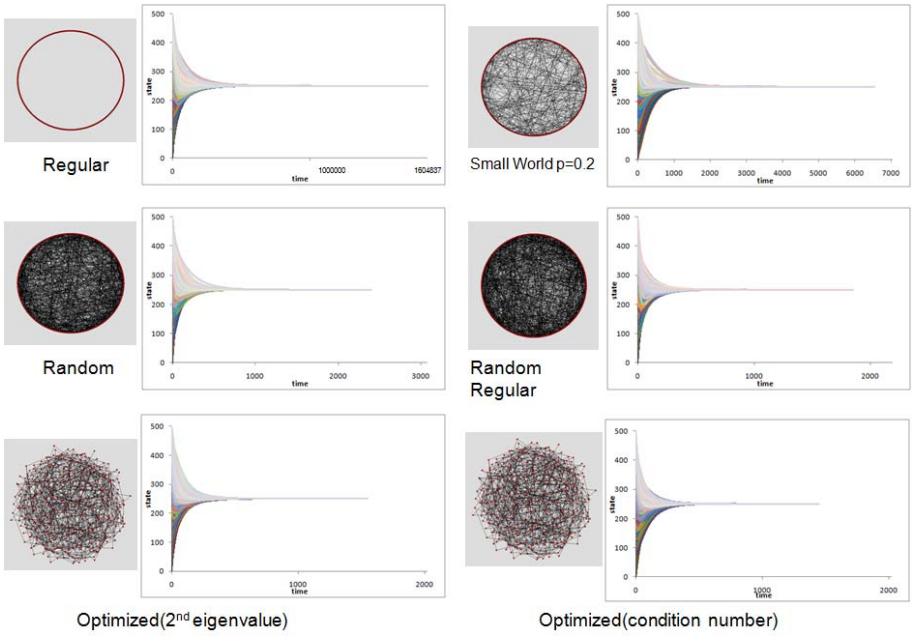


Fig. 11. Network convergence process

This means the collective dynamics converge to the average of the initial states of all agents, the results of the convergence process of the each networks are shown in Figure 11.

Regular networks, the algebraic connectivity is very so low that the convergence time is very much time step. It takes a lot of time. small-world networks (represented $p = 0.2$) is faster convergence time compared to the regular network, which is 6532 convergence time step.

For $p = 1$, the random network, the time step of convergence is 2393 time step, random network is one of the fastest networks in the models based on the link probability p.

Random regular network has higher algebraic connectivity than random networks, so convergence becomes faster, the time is 1848 step. Optimized network(optimized by λ_2) convergence time is 1542 time step, which is faster than random regular network which is fastest in the previous network models. We can see that the network optimized by only λ_2 has better consensus and synchronization property than random regular network. Optimized network(optimized by condition number) convergence time is 1443 time step, which is faster than the optimized network(optimized by λ_2). The convergence time of optimized network(optimized by condition number) is fastest of all the networks we compare. As we see so far, we can see that the algebraic connectivity is greater in evolutionary optimized networks than random regular(Ramanujan graph) networks which are the highest algebraic connectivity networks in the previous network

models(regular network, random network, small-world network and random regular network). And optimized networks have far better algebraic connectivity and Q(condition number) values than random regular networks. These property we examine also corresponds to the actual convergence time, the convergence time of optimized network(optimized by condition number) is fastest of all the network models. This optimized networks are suitable to call "optimal", which has best convergence property for consensus and synchronization.

Optimal networks we obtained in this study, show better synchronization and consensus property to see the convergence speed and network eigenvalues. In the previous study, network model has been created under the regular rules, and investigated their characteristics. But in this study, network is evolved to suit the characteristics of the objection by evolutionary algorithm and we create optimized network. Consensus and synchronization problem is closely related to the variety of issues such as collective behavior in nature, the interaction between agents and factor, as a matter of the robot control and many agents coordination, understanding the property of nature synchronization and building efficient wireless sensor networks, etc. Consensus and synchronization problem is associated with various issues, therefore, the optimal networks which we proposed indicate its significance and effectiveness as one of the best network structures.

6 Conclusion and Remarks

In this study, we proposed the optimal networks based on evolutionary algorithm which consider link density and Laplacian matrix eigenvalue. We show that the 2nd smallest eigenvalue and Q(condition number) are greater in evolutionary optimized networks than random regular(Ramanujan graph) networks which are the highest algebraic connectivity networks in the previous network models(regular network, random network, small-world network and random regular network). And the convergence speed is faster in evolutionary optimized networks than random regular(Ramanujan graph) networks which are currently known as the best consensus and synchronization networks in the previous network models. We can conclude optimal networks are the most suitable to the property of consensus and synchronization. Consensus and synchronization problem is closely related to the variety of issues, so the optimal networks which we proposed have significance to design and consider about the network system and society.

References

1. Neda, Z., Ravasz, E., Brechet, Y., Vicsek, T., Barabasi, A.L.: The sound of many hands clapping. Nature 403, 849–850 (2000)
2. Strogatz, S.H.: From kuramoto to crawford: exploring the onset of synchronization in populations of coupled oscillators. Phys. D 143(1-4), 1–20 (2000)
3. Olfati-Saber, R., Murray, R.M.: Consensus problems in networks of agents with switching topology and time-delays. IEEE Transactions on Automatic Control 49(9), 1520–1533 (2004)

4. Olfati-Saber, R., Fax, J.A., Murray, R.M.: Automatic on Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE 95, 215–233 (2007)
5. Ren, W., Beard, R.W.: Distributed Consensus in Multi-vehicle Cooperative Control. In: Communications and Control Engineering. Springer, Heidelberg (2008)
6. Strogatz, S.H.: Exploring complex networks. Nature 410(6825), 268–276 (2001)
7. Kauffman, S.A.: The Origins of Order: Self-Organization and Selection in Evolution. Oxford University Press, Oxford (1993)
8. Barahona, M.: Synchronization in small-world systems. Physical Review Letters 89(5), 54101 (2002)
9. Erdös, P., Rényi, A.: On random graphs. I. Publ. Math. Debrece 6, 290–297 (1959)
10. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature 393(6684), 440–442 (1998)
11. Barabási, A.L., Albert, R.: Emergence of scaling in random networks. Science 286(5439), 509–512 (1999)
12. Donetti, L., Hurtado, P.I., Munoz, M.A.: Entangled networks, synchronization and optimal network topology (October 2005)
13. Xiao, L., Boyd, S.: Fast linear iterations for distributed averaging. Systems & Control Letters 53(1), 65–78 (2004)
14. Sato, H., Isao, O., Shigenobu, K.: A new generation alternation m odel of genetic algorithms and its assessment. Journal of Japanese Society for Artificial Intelligence 12(5), 734–744 (1997)
15. Hovareshti, P., Baras, J.: Consensus problems on small world graphs: A structural study. Technical report, Institute for Systems Research (October 2006)
16. Kar, S., Aldosari, S., Moura, J.: Topology for distributed inference on graphs. IEEE Transactions on Signal Processing 56(6), 2609–2613 (2008); see also Acoustics, Speech, and Signal Processing
17. Pikovsky, A., Rosenblum, M., Kurths, J.: Synchronization: A Universal Concept in Nonlinear Sciences. Cambridge Nonlinear Science Series. Cambridge University Press, Cambridge (2003)
18. Bollobas, B.: Random graphs. Cambridge Univ. Pr., Cambridge (2001)

Geospatial Analysis of Cooperative Works on Asymmetric Information Environment

Tetsuya Kusuda[1,2] and Tetsuro Ogi[1]

[1] Keio University, Graduate School of System Design and Management,
4-1-1 Hiyoshi, Kouhoku-ku, Kanagawa, 223-8526 Japan
[2] NTT Data Corporation,
3-3-9 Toyosu, Koto-ku, Tokyo, 135-8671 Japan
kusuda@z7.keio.jp, ogi@sdm.keio.ac.jp,
kusudat@nttdata.co.jp

Abstract. In the so-called Information-Explosion Era, astronomical amount of information is ubiquitously produced and digitally stored. It is getting more and more convenient for cooperative works in the sense of information sharing. Information aggregation systems are widely available and search engines are the most useful tools for finding resources on the internet. However, the use of information is not sufficient for cooperative works such as decision making. This is partly because, as the systems get larger, the stakeholders of the systems increase and they are on Asymmetric Information Environment (AIE). We do not share everything on the network. In this paper, we present the importance of AIE-oriented systems design for cooperative works using simulations and geospatial analysis on Multi-Agent Disaster Evacuation Model. As a result, using small data like positioning information and status information of agents, we can visualize the situations and take effective actions for cooperative works on AIE. Communication techniques on AIE such as signaling, positioning information monitoring and positioning information screening are effective for geospatial analysis of cooperative works on AIE. In conclusion, we can increase values from information flows by increasing effective actions for cooperative works using AIE-oriented systems design. Real field experiments are to be followed in our plan.

Keywords: Geospatial Analysis, CSCW, Collective Systems, Asymmetric Information Environment, Information flows, Multi-agent simulation.

1 Introduction

In the so-called Information-Explosion Era [1], astronomical amount of information is ubiquitously produced and digitally stored. Not only human activities on the internet but also automated systems are producing digital data in the world. Sensor networks, video surveillance, system logs are working perpetually. Information flows create values in our society. Search engines are the best solutions that make information flows and create values on the internet. Sensor networks are valuable because they automatically measure specific data and make information flows. It is getting more

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 336–345, 2010.

and more convenient for cooperative works in the sense of information sharing. Information aggregation and management systems like GIS (Geographic Information System) are widely available and search engines are the most useful tools for finding resources on the internet. However, the use of information is not sufficient for cooperative works such as decision making. This is partly because, as the systems get larger, the stakeholders of the systems increase and they are on Asymmetric Information Environment (AIE). We don't share everything on the network for collaboration. We don't need to share everything because the information needs are different from each other by roles and situations. We can't share the information sometimes due to network troubles at disasters.

In this paper, we present the importance of AIE-oriented systems design for cooperative works using simulations and geospatial analysis on Multi-Agent Disaster Evacuation Model. As a result, using small data like positioning information and status information of agents, we can visualize the situations and take effective actions for cooperative works on AIE. Communication techniques on AIE such as signaling, positioning information monitoring and positioning information screening are effective for geospatial analysis of cooperative works on AIE. In conclusion, we can increase the values from information flows by increasing effective actions for cooperative works using AIE-oriented systems design. Real field experiments are to be followed in our plan.

2 Related Works

In geospatial analysis and GIS field, systems are getting larger. Some countries are promoting NSDI (National Spatial Data Infrastructure [2]) concept to structure nation-level information aggregation systems. However, orchestrating multiple government sectors to share their information is a tough job because of AIE reasons. Current solutions for NSDI are sharing fundamental data and metadata [3] to search the contents efficiently.

Cooperative work has been studied as CSCW (Computer Supported Cooperative Work) field that is an interdisciplinary research area for social psychologists, sociologists, and computer scientists. CSCW concept is commonly defined by time-space matrix [4]. So geospatial analysis is well matched with CSCW concept. As the network infrastructures have been developed and systems are getting larger, the number of stakeholders tends to increase. AIE-oriented systems design is needed for a large-scale CSCW system like a Disaster Management and Support System [5]. In recent years, collective systems have gained considerable attention in large systems design with considering stakeholders as adaptive agents to establish coordinated systems from the bottom up [6].

Asymmetric Information has been studied in the field of contract theory in economics [7]. Information asymmetry is the situation that at least one party does have some information which the others do not upon transactions. There are two kinds of problems in this situation that are moral hazard and adverse selection. Moral hazard is the problem if information asymmetry happens after the contract. Adverse selection is the problem if information asymmetry exists before the contract. An example of moral hazard is employer's ignorance of the lack of employee's diligence after the

employment. An example of adverse selection is employer's ignorance of the lack of employee's ability before the employment. It is known that monitoring technique is effective to cope with moral hazard problem and that signaling and screening techniques are effective against adverse selection problems. In this paper we tried to apply these techniques to systems design of multi-stakeholders' huge systems as AIE-oriented systems design methods. We enlarged the concept of asymmetric information to "Asymmetric Information Environment" because it is not only discussed on contract theory but also on communications theory.

3 AIE Example and Simulation Model

Information flows create values for society and AIE is the source of information flows. Because information flows stem from the information gaps on AIE as water flows from higher to lower places. The problem of AIE emerges where the stakeholders of the systems are not conscious of their differences on AIE and just promoting information sharing. The differences of information might make misunderstandings and sometimes ignoring the differences causes the problem.

3.1 Real-Time Disaster Management and Support System

At first, we consider Real-time Disaster Management and Support System (R-DMSS: Fig.1) for example. R-DMSS is a network system that connects the emergency headquarters and the disaster sites. GIS is used by the central user for information aggregation and management. This system is supporting the cooperative works between emergency headquarters and disaster sites.

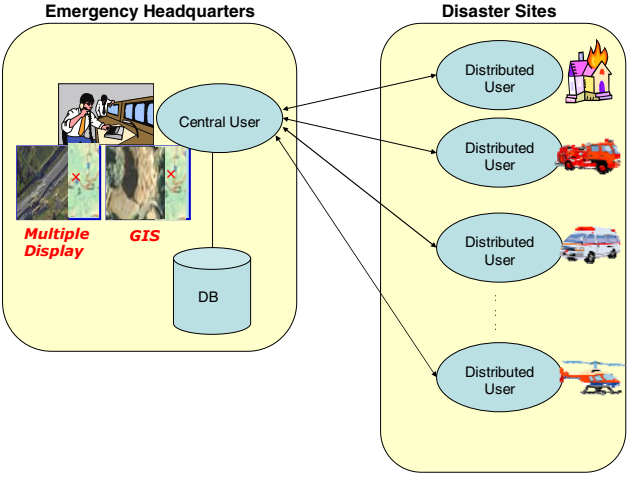


Fig. 1. Real-time Disaster Management and Support System

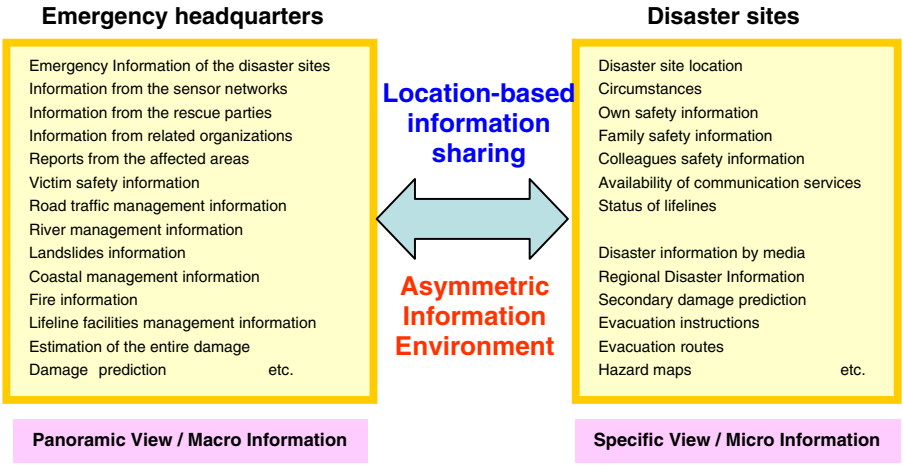


Fig. 2. Information gaps on Asymmetric Information Environment

As it is shown in Fig.2, location-based information sharing is useful on AIE, but information gaps inevitably exist. While cooperative works are conducted between emergency headquarters and disaster sites, the information they need are different from each other because of the differences of their roles and situations. Emergency headquarters need panoramic view and macro information. On the other hand, disaster sites need specific view and micro information. All the information are valuable only when they produce decisions for actions. We have to design the system so that information flows create values like immediate actions to rescue injured people.

3.2 Simulation Model

We analyzed the system on Multi-Agent Disaster Evacuation Model (Fig.3).

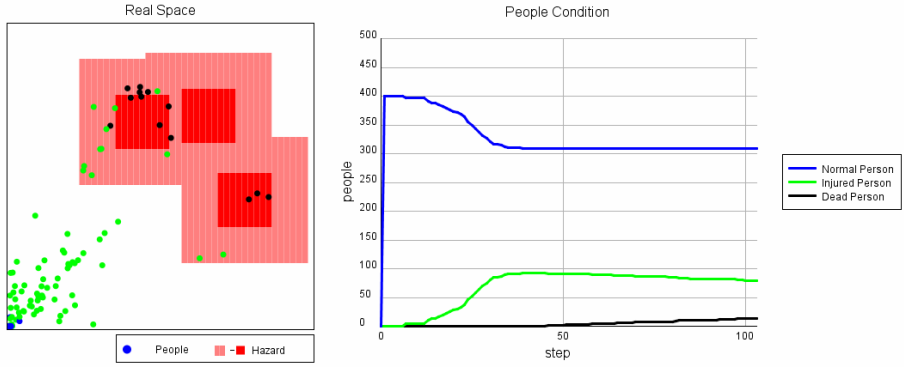


Fig. 3. Multi-Agent Disaster Evacuation Model

Table 1. Simulation Model Specification

Model Summary	People evacuate from the disaster site to the shelter on the simulation space.
Space	50×50 square area
People	100 to 500 people (specify the number from the control panel and randomly placed on the space)
Hazard	1-5 units (specify the number and randomly placed on the space) 8×8 square area: the core of the hazard 20×20 square area: the periphery of the hazard
Shelter	The shelter is at the lower left corner. People know it.
Rules	・To shelter people evacuated while damaged from the hazards ・the core of hazard affects people more than the peripheral ・According to the damage level, the condition of the people changes like normal (blue) → injured (green) → dead (black) ・People try to avoid the core of the hazard ・Movement of people is dwindling due to cumulative damage
Emergency Headquarters	track the location of people in some extent
Simulator	artisoc textbook, KOZO KEIKAKU ENGINEERING Inc. [8]

The specification of the simulation model is shown in Table 1. Using this model, we have already found the following [5].

- Using small data like positioning information and status information of agents, we can visualize the situations and take effective actions for cooperative work on Asymmetric Information Environment.

In this paper, we extended the model and investigated communication techniques on AIE by simulations. The simulation test methods were as follows.

Simulation 1

(1) Emergency headquarters can track the location of people randomly, 10% at a step.
(2) Signaling technique Test: Injured person sends help alert when his damage level is increased. Individual differences for the decisions are randomly added.
(3) Positioning information monitoring technique Test: Emergency headquarters monitor the location of each person, compared to the previous location if he does not move any more. The motionless person detected is the target of rescue.

Simulation 2

(1) Emergency headquarters can track the location of people who have the positioning terminals. The terminal penetration (TP) is the parameter of the simulation.
(2) Positioning information screening technique Test: Emergency headquarters identify rescue target area by screening of injured person's trails from all the trails.
(3) To verify the efficacy of screening method, we counted the dead persons on the screened area for 10 times of simulations for each TP (10%, 20%, 25%, 50%, 75%).

4 Results and Discussions

The results of the simulations are as follows. We found that the tested communication techniques are effective on AIE.

4.1 Simulation 1

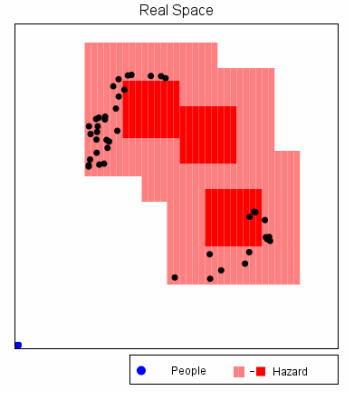


Fig. 4. Real Space View (step 200, response 10%)

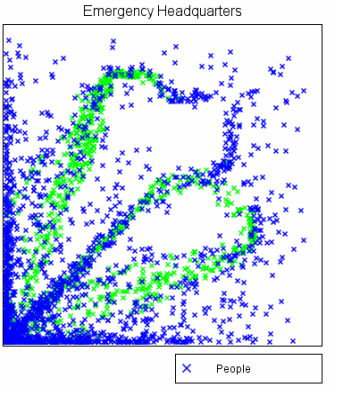


Fig. 5. Emergency Headquarters' View (step 200, response 10%)

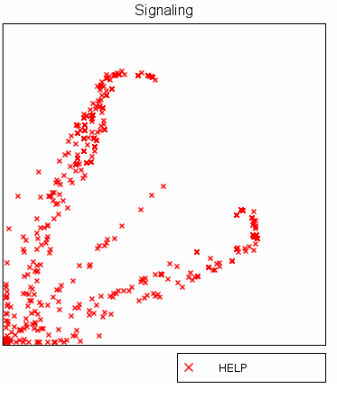


Fig. 6. Signaling (step 200, response 10%)

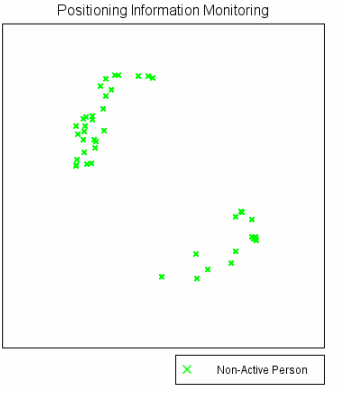


Fig. 7. Positioning Information Monitoring (step 200, response 10%)

Spatial Analysis. Comparing Fig.6 and Fig.7, signaling was more redundant than monitoring because the latter pointed out the same result of the dead persons as is shown in Fig.4. The reason of the redundancy is that individual differences for the decisions are randomly added according to the damage levels in the signaling case. Signaling is a subjective method and the best way to tell others of one's reality. However, the realities are different from each other on AIE. So signaling alerts include

some noises, and in the worst case, they cause moral hazard problem. On the other hand, positioning information monitoring is an objective method and partly eliminates AIE problems like moral hazard.

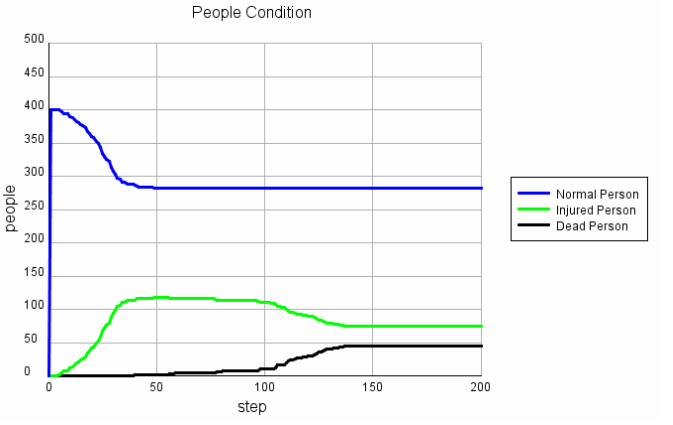


Fig. 8. Timeline of the numbers of the injured and the dead

Timing Analysis. Fig.8 shows the numbers of the injured and the dead. If we can rescue people before 100 step, the damage would be relatively small. If it would take 40 steps for rescue actions after the alert of signaling or monitoring, the alerts in the left bottom box in Fig.9 (0<MST<40, 0<SST<40) are useless. The alerts in the right bottom box (0<MST<40, 40<=SST) are effective owing to signaling alerts. The alerts in the right top box (40<=MST, 40<=SST) are also effective to start rescue.

Fig. 9. Timing analysis: Alerts Starting Times before Time of Death

From the result, we found that: (1) Signaling contains noises because of the reasons such as moral hazard but it creates valuable information flows for quick actions. (2) Monitoring partly eliminates AIE problems but it sometimes causes delayed actions.

4.2 Simulation 2

Fig.10, Fig.11 and Fig.12 show the results of positioning information screening test. In the simulations, we considered the reality of terminal penetration (TP). Only selected people who have the positioning terminals can be tracked by emergency headquarters (the middle figures). We extracted the trails of injured persons (green area of the right figures) by the screening technique and seemed the green area as the targeted rescue area. Comparing the green screened area of trails and the positions of dead persons (black dots in the left figures), we investigated the average coverage of the positions of dead persons by the green area. We tried 10 times of simulations for each TP (10%, 20%, 25%, 50%, 75%). As a result, we have got Fig.13.

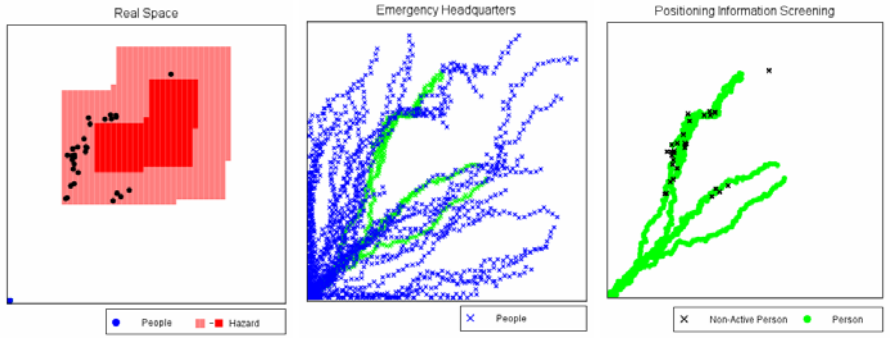


Fig. 10. Positioning Information Screening (step 200, Terminal Penetration 10%)

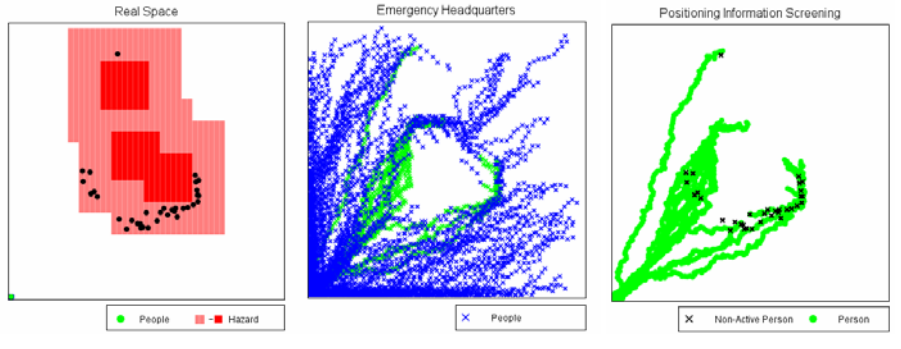


Fig. 11. Positioning Information Screening (step 200, Terminal Penetration 25%)

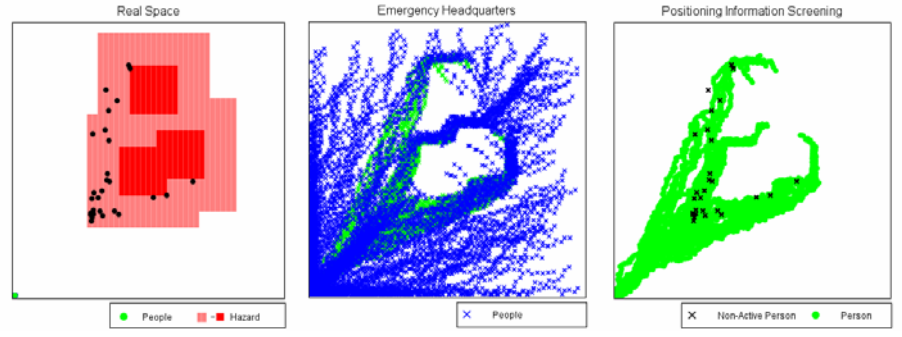


Fig. 12. Positioning Information Screening (step 200, Terminal Penetration 50%)

Analysis

(1) If TP >= 25% i.e. more than one terminal device available for every four persons, more than 90% coverage was obtained. When TP = 20%, the coverage was 85%. It seems like a Pareto principle's curve. Using small data like positioning information and status information of agents, we can visualize the situations and take effective actions for cooperative works on AIE.
(2) If we use the positioning information monitoring method in Fig.10, only 10 % of dead persons could be detected stochastically. It is not an effective solution to grasp the panoramic situation of the disaster. We have to select the solutions according to the case.

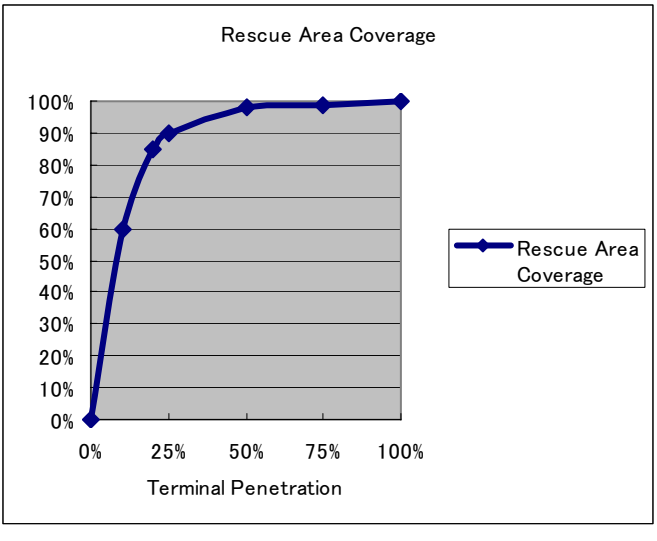


Fig. 13. Rescue Area Coverage

(3) From the results, we also found that the hazards are one of the constraints for the selection of the evacuation trails. If victims could take every path to the shelter, the coverage would be lower because everyone takes its path randomly. This analysis shows that we can adequately control people with constraints at disaster. It suggests that the clarification of evacuation routes is very important for R-DMSS. Education, drills and tools such as hazard maps also could be recommended solutions for safety measures.

5 Conclusions

In conclusion, we have obtained the following from simulation experiments:

(1) Using small data like positioning information and status information of agents, we can visualize the situations and take effective actions for cooperative works on Asymmetric Information Environment.
(2) Communication techniques on AIE such as signaling, positioning information monitoring and positioning information screening are effective for geospatial analysis of cooperative works on AIE. Because they can create information flows to create actions. We have to select the techniques according to the case.

We can increase values from information flows by increasing effective actions for cooperative works using AIE-oriented systems design.

In future, we will make the simulation model more complex by adding more realities such as maps, route guidance information for evacuation, multiple shelters, rescue activities, hazard prediction information and other factors. More communication techniques on AIE should be tested including signaling from emergency headquarters. Real field experiments are to be followed in our plan.

Acknowledgments. This research was supported by G-COE (Center of Education and Research of Symbiotic, Safe and Secure System Design) program at Keio University.

References

1. Kitsuregawa, M., Matsuoka, S., Matsuyama, T., Sudoh, O., Adachi, J.: Cyber Infrastructure for the Information-Explosion Era. Journal of Japanese Society for Artificial Intelligence 22(2), 209–214 (2007) (in Japanese)
2. What is the world trend in NSDI? - Towards the Construction of Sustainable Geospatially Enabled Society. In: International Symposium on NSDI, CSIS. The University of Tokyo (2009), http://i.csis.u-tokyo.ac.jp/event/20090608/
3. Geospatial Metadata, http://www.fgdc.gov/metadata
4. Johansen, R.: GroupWare: Computer Support for Business Teams. The Free Press, New York (1988)
5. Kusuda, T., Ogi, T.: A study of positioning information utilization on real-time network systems for safety measures. IEICE technical report 109(250), 17–20 (2009) (in Japanese)
6. Namatame, A.: Adaptation and Evolution in Collective Systems. World Scientific Pub. Co. Pte. Ltd., Singapore (2006)
7. Kambe, S.: A Primer in Game Theory and Informational Economics. Nippon-Hyoron-Sha Co.Ltd., Tokyo (2004) (in Japanese)
8. Yamakage, S.: Modeling and Expanding Artificial Societies - Introduction to Multi-Agent Simulation with artisoc. Kozo Keikaku Engineering Inc., Shosekikobo Hayama Publishing Co. Ltd., Tokyo (2009)

Emergent Stock Market Behaviour from a Multitude of Simple Agents

Volker Nissen and Danilo Saft

Ilmenau University of Technology, Chair of Information Systems in Services,
PF 10 05 65, D-98684 Ilmenau, Germany
www.tu-ilmenau.de/wi2

Abstract. In our work the focus is on emergent behaviour in large groups of stock market participants. We do not assume that market participants take rational investment decisions based on full information as would be the case in established views of the capital market. Consequently, the market is not modelled top-down with mathematical equations. Instead, trading decisions and market behaviour are the result of individual participants reacting to stock price and price changes. Each participant is modelled as a fuzzy agent that behaves according to simple trading rules. The research goal we pursue is to increase our understanding of the relationship between simple, swarm-like individual trading behaviour and its macroscopic effects at the market level.

Keywords: Emergence, stock market, multi-agent system, swarms, fuzzy sets.

1 Short Introduction to Stock Market Models

Traditional models of financial markets take a macroscopic perspective, modelling market behaviour with mathematical equations. The underlying assumption in the classical case is the efficient market hypothesis (EMH), which suggests that all relevant information is instantly available to all market participants, who then make well-informed, rational decisions about their investments. From this, market price is a result of the distribution of expectations in the market regarding future yield [1]. Frequently, a normal distribution of these expectations is assumed and only random influence can lead to a short-term above-average performance of individual market participants. Thus, stock prices display a random path (Random Walk Theory) [2].

Reality is apparently different. Empirical studies have confirmed correlations between historic and current price levels for stocks [3]. Results in fractal mathematics have underlined that the random walk theory does not apply and structures can be found in stock price graphs [1] [4]. More recent models, such as the synergetic capital market model from Landes/Loistl [15], suggest that a micro-level examination of the entities and processes in share trading is required. However, the synergetic capital market model is complex [15, pp. 319 – 345]. Moreover, fundamental influences on markets play an important role, which is not the assumption underlying our work.

In this paper we argue for a bottom-up model that focuses on individual market participants and draws a remote parallel to biological swarms. The assumption here is

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 346–357, 2010.

that at least the private traders act more like members of a herd rather than analyzing fundamental influences on the market to arrive at their trading decisions. Market behaviour then arises as an emergent phenomenon at the macroscopic level. Section 2 gives a short introduction to concepts central to our research. In section 3 the experimental setting is highlighted. Section 4 includes experimental results and their interpretation. We conclude with lessons learned and research implications.

2 Swarm Behaviour and Stock Markets

Many animals in nature, such as birds, fish and ants, operate in swarms, i.e. they form large groups of individuals that display coordinated movements. While the animals themselves are quite limited in their abilities and the rules of coordination are simple, complex swarm behaviour can be generated at the macroscopic level since each individual generates an indirect force on all other individuals and is itself under multiple influences from other swarm members.

Swarms have recently received much attention in the context of artificial life and artificial intelligence [5] [6] [7] [8] due to their emergent behaviour. Robustness and the ability for self-organisation are important characteristics of swarms. These features make artificial swarm-like systems interesting for practical applications, where autonomy and fault tolerance are important. Moreover, swarms may be seen as an example for bottom-up simulations that model real systems not at the macroscopic level using mathematical equations but focus on the microscopic parts of the system, their characteristics and microstructure. This is the view on stock markets adopted in this paper. It is, in fact, typical for agent-based computational economics [14] [16] [17]. For an overview of agent-based models of financial markets see [18].

We take up the position of Schleis [10], who describes the population of stock market participants as a social being in its own right, whose members influence and control each other particularly through the pricing mechanism. Combining this viewpoint with the idea of a bottom-up market model as discussed in [15], one arrives naturally at the research goal to construct a micro-level model of a capital market containing a large number of trader entities with simple behaviour, influencing each other indirectly through their trading decisions and the resulting stock price level. Our focus is on the relationship between individual trading behaviour and macroscopic stock price movements. It is important to underline that we do not aim to forecast stock prices nor do we attempt to generate the historical curve of a particular stock.

Moreover, we believe it is unnecessary to assume the typical BDI-agent structure and complex reasoning and cooperation processes of common multi-agent simulations to achieve this goal. The emergent creation of complex macroscopic price movements by a multitude of very simple agents would give a hint that trading decisions in real markets are often taken in a much simpler fashion than is commonly thought. We further believe it is not required to assume external market forces or changes of fundamental data to create major changes of stock prices. This in turn would induce that forecasting stock market developments is a hopeless task.

3 Bottom-Up Simulation of a Stock Market

3.1 Structure of the Fuzzy Trader Agents

Our stock market is populated by a large number of simple trader agents that buy and sell a single stock. 1000 agents are employed in the simulation. This quantity was determined empirically during initial tests. It is sufficient to achieve a well-distributed diversity in the agent population, but avoids excessive computational requirements.

Market participants in our simulation do not perform complex analyses of macro-economic figures before they act. Rather, they evaluate stock price and the trend in prices over some period of time and then decide whether to trade based on behaviour that is coded in a fuzzy rule base and inference mechanism.[1] Thus, market participants are modelled as stimulus-response agents. Figure 1 gives the structure of a trader agent, which is essentially the structure of a Mamdani-style technical fuzzy controller.

Crisp (not fuzzy) input (price level, trend in prices) is fuzzyficated, i.e. mapped on fuzzy sets. Then, the compatibility of the facts with the conditions of rules in the knowledge base is checked. The result is in each case a real number in the interval [0,1]. For each rule, the results of individual conditions are aggregated to an overall compatibility for the condition part of the rule. A rule is activated when its condition part is fulfilled to an extent greater than zero. Several rules may be activated in parallel. A fuzzy inference mechanism (the well-established max-min inference) then maps the input to the output of the fuzzy trader agent. In a last step, the fuzzy output set concerning the trading decision (buy, hold, sell) is converted to a crisp decision by applying standard centre-of-gravity defuzzyfication.

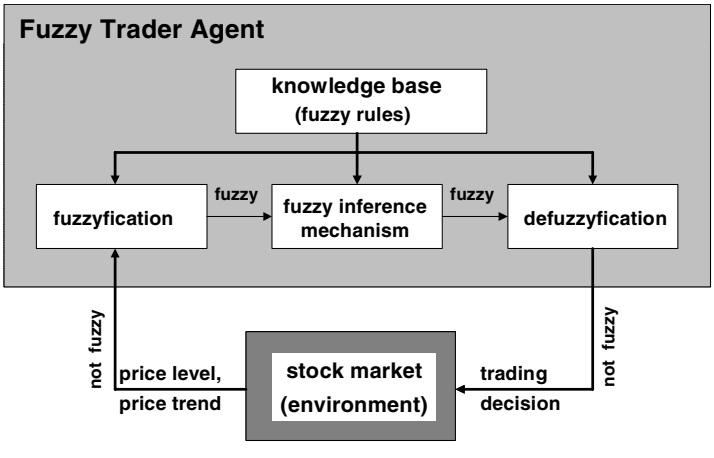


Fig. 1. Structure of a fuzzy trader agent. Crisp information on price level and the trend in prices is the input while a decision to buy, hold or sell a certain amount of stock is the output.

Using fuzzy set theory [12] [13] to model the trader agents has several advantages. First, fuzzy rules offer a simple yet elegant way to explicitly code human knowledge. Second, only a few rules suffice to generate sensible agent response in all relevant

[1] Agents could also make use of trading volume information, but for the experiments here we abstract from volume figures, as the fundamental principles of trading remain the same.

contexts of our model. Third, fuzzy systems are generally robust and display smooth behaviour patterns in dynamic environments [11]. Fourth, the behaviour of agents can be changed individually by adapting fuzzy sets or rules in the knowledge base.

3.2 Further Model Details at the Micro-level

The input of each trader agent in our model are price level and trend in prices, both normalized to the range [-1, 1]. The output value is interpreted as the decision to buy, hold or sell stock. Figure 2 displays the fuzzy sets for input and output.

The real valued function $\mu_{\tilde{A}} : X \rightarrow [0,1]$ is the membership function. Herein, a value $\mu_{\tilde{A}}(x) = 0$ means that x does not belong to the fuzzy set $\tilde{A}$, while a value $\mu_{\tilde{A}}(x) = 1$ indicates full membership. Values in the interval $0 < \mu_{\tilde{A}}(x) < 1$ indicate a partial membership of x in the set $\tilde{A}$. Based on the fuzzyficated inputs the inference mechanism of each fuzzy agent generates a crisp value in the interval [-1, 1] for the output. This value forms the basis for the trading decision of the respective agent.

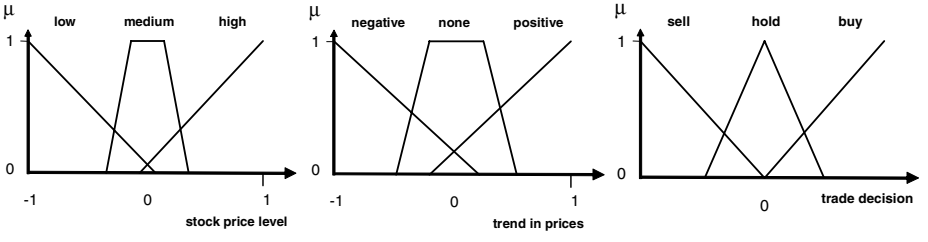


Fig. 2. Fuzzy sets (linguistic terms) for input and output variables of fuzzy trader agents

The precise geometry of each input fuzzy set can vary between agents to emulate different market assessments as will be described later. However, all agents have an identical knowledge base of rules as given in table 1. Agents generally show market-conforming behaviour, thus displaying swarm-like coordination through the stock price. This is in accordance with empirical studies about human behaviour in complex, non-linear systems where test subjects frequently followed an ad-hoc hypothesis of linear trend [1, pp.126]. Moreover, Schleis argues from a psychological position that crowds of people tend to display self-enforcing feedback processes of euphoria or panic [10, pp.29].

Table 1. Rule base of fuzzy trader agent (rules identical for all agents)

IF Price	AND Trend in Prices	THEN Trade Decision
low	Negative	buy
medium	Negative	sell
high	Negative	sell
low	None	hold
medium	None	hold
high	None	hold
low	Positive	buy
medium	Positive	buy
high	Positive	sell

A trader will only change his trading decision against the current market trend when new information with sufficient intensity is available that indicates a probable change in the stock price pattern. So, when the trend in prices is still positive but the price level is considered "high" by the agent, it will start selling. It will start buying when the price trend is still negative but the price level is already considered "low".

It is assumed that trading is always possible. This is, of course, a simplification over the real stock market where limits, such as stop-loss, play an important role and one might not be able to sell stock at a given time because of a lack of demand. However, such additional constraints would only complicate the model without adding value to pursuing our current research goals.

No central market maker is employed in our model who decides about the stock price. However, the basic market mechanism is present, i.e. the stock price will change in proportion to direction and volume of the overall trading decisions.

3.3 Simulation at the Macro-level

The stock market simulation is processed in discrete time steps. These steps are conceptually comparable to the regular time interval for the price determination in real stock markets. For example, this price determination happens every second for the *Deutsche Aktienindex* DAX. At the macroscopic level, the inputs (price level, trend in prices) for all agents are calculated, using the current status of the stock market system and the outputs (trading decisions) of the agents. The trend in prices Δk of trading cycle t is calculated at

$$\Delta k_t = \frac{M_t^{buy} - M_t^{sell}}{M_t^{buy} + M_t^{sell}} \tag{1}$$

where M_t^{buy} is the total trade volume of stock bought in period t while M_t^{sell} is the total trade volume sold in period t. At this stage, we relax the requirement that both volumes must be identical, thus avoiding the necessity for bookkeeping of individual stock volumes for one thousand trade agents. Instead, we assume some trading institution as part of the market that is always prepared to buy and sell stock at the current price in the required amount. This simplifying assumption will be removed in future research, while it currently helps to focus on the aspects of interest. It should be noted that in real markets such asynchronous trade situations can indeed occur, for instance in the case of short sales by hedge funds. The initial Δk_0 is set to the value of zero (neutral). The stock price k_t at the end of trading period t is then given as

$$k_t = k_{t-1} + \Delta k_{t-1} \tag{2}$$

The calculation of the relevant stock price level p_t as one of the input variables for the trading agents varies between the different simulation experiments. However, it is not identical to the stock price k_{t-1} at the end of the previous trading period. Instead, agents individually calculate an average price over some historic period and use this in their trading decision. The length of this historic period s is a random variable that is determined independently once for each agent at the start of the simulation, just as individual traders in real markets take individual perspectives on past prices. In our

experiments it is assumed that this random variable is normally distributed. If *s* is small, then an agent ignores most of the price history in its calculation of the input "stock price level".

The 1,000 fuzzy trader agents communicate only indirectly through the stock price k_t that is the result of aggregated trading decisions of the individual agents. Trading does not necessarily occur in each period. Instead, trading frequency *f* is a normally distributed random variable, determined once for each agent. Thus, different trading attitudes, such as day traders and long-term investors can be emulated.

In addition to the historic period *s* and the trading frequency *f,* a third parameter is of major importance for the simulation: the diversity *d* of market assessments in the population of agents. In real markets, some traders are more risk-averse than others, thus their individual assessment of a given market situation can differ significantly. This is emulated by varying the geometry (position and width) of the fuzzy sets for each of the two input variables of a trader agent within predefined ranges. Thus, the assessment of stock price level and trend in prices varies between different agents, influencing their individual decision to buy, hold or sell stock. This variation of fuzzy sets is done at the start of the simulation individually and once for each agent using a $(0,\sigma)$-normally distributed random variable. The std. dev. of the random variable can be used to create different behavioural diversity in the population of trader agents.

With *s*, *f* and *d* some useful parameters are available to influence the individual behaviour of the fuzzy trader agents and analyse the relation of microscopic behaviour patterns and macroscopic effects. When looking at the effects in section 4 it is worth mentioning that random numbers are only created and applied during initialisation, but the simulation itself is deterministic. Please note that the trader agents do not adjust themselves to the system output through learning[2]. All parameters are initialised and thereafter remain static during the course of the simulation run.

4 Simulation Experiments

For each experimental setting 20 runs with different random number seeds were performed. A single run consists of 300 trading periods. As averaging over different runs is not meaningful in this context, we present graphs and discuss results of individual runs that display 'typical' behaviour for the respective parameterisation. It is acknowledged that this choice is somewhat subjective. The initial price level and trend in prices in all experiments are set to zero (neutral), serving as a baseline reference for the following price movements.

It should be kept in mind that the regular patterns described below are all created without exogenous shocks to the stock exchange system. Moreover, agents do not coordinate themselves directly through communication or a central coordination agent. They only observe other agents behaviour indirectly through the price level and trend in prices and apply simple trading rules, representing their market assessments.

[2] Individual agent learning, e.g. by creating new behavioural rules, looks like a promising research path, though. Future work will take up this issue.

4.1 Experiment 1

Agents calculate the price level input p_t as the average stock price within their relevant historic period s ($s \in [1 \ldots t-1]$). k_i denotes the stock price in period i.

$$p_t = \frac{\sum_{i=t-s-1}^{t-1} k_i}{s} - k_0 \tag{3}$$

Furthermore, trading occurs deterministically in every period and the diversification of market assessments in the population is initially low. This allows us to better isolate and analyse the influence of s on the macroscopic level. Figures 3 (a)-(d) demonstrate the effect of raising the expectation of s with its std. dev. remaining at zero, meaning that agents include more historic price values in their price level calculation, but do so in an identical way. The resulting macroscopic effects are an increase in amplitude of the stock price movement with time and a proportional prolongation of each price cycle. As s is raised, more values enter the calculation of the agents' stock price level. Thus, the influence of short-term price movements diminishes and the inertia of the price level rises, leading to later reactions of agents to current stock price movements and, thus, the visible macroscopic effects.

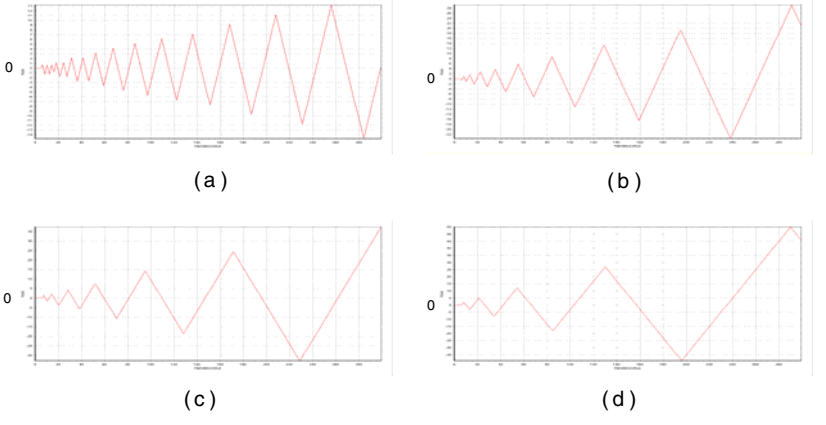


Fig. 3. Results with behavioural agent diversification $d = 0.1$ (low), trading in each period and s-value expectations of 10% (a), 20% (b), 30% (c) and 50% (d) of simulation periods. The curves display stock price k_t over time during a complete simulation run.

When the diversity of market assessments in the agent population is raised *ceteris paribus (c.p.)* (meaning more behavioural diversification), then this smoothens the stock price curve at its turning points and simultaneously softens the price cycles (figure 4). Now, as the market assessments at each point in time are more diverse, more agents may act in opposition to the general trend in the population, thus indirectly convincing other agents to leave their current trading positions. This leads to less abrupt changes of stock price at the turning points of the price pattern and also shortens corresponding price cycles by lowering the amplitudes.

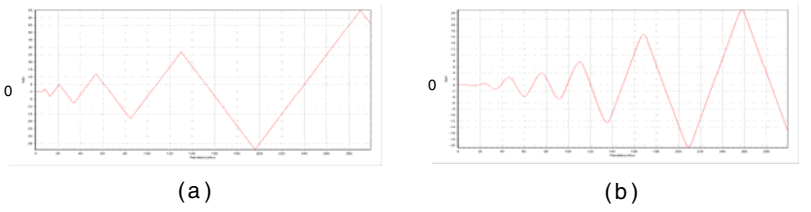


Fig. 4. Results for *s*-value expectation of 50% and behavioural agent diversification $d = 0.1$ (a) and $d = 0.5$ (b). Rest of parameters as in figure 3

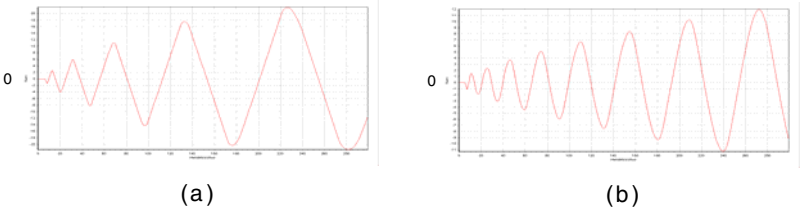


Fig. 5. Results for *s*-value expectation of 50% with a standard deviation of 10% (a) and 30% (b). Rest of parameters as in figure 3

A similar effect can be achieved *c.p.* by introducing a standard deviation for *s*, as can be seen in figure 5. Now, the behavioural diversification in the population is low, but agents apply their trading rules to different price levels, resulting again in different market assessments, thus smoothing the stock price curve at the turning points, but also shortening the price cycles.

4.2 Experiment 2

In the second experiment, agents calculate the price level input p_t as the average stock price within their historic period s ($s \in [1 \ldots t-1]$), but with reference to the stock price at the beginning of this period. k_i again denotes the stock price in period i.

$$p_t = \frac{\sum_{i=t-s-1}^{t-1} k_i}{s} - k_{t-s-1} \tag{4}$$

Here, an interpretation of results is much more difficult, as each agent deduces an *individual* stock price from the average price over its historic period, leading to very different inputs, and consequently trading decisions, for agents.

The first series of simulation runs has identical parameterisation as in the previous experiment with focus on the length s of the historical price period. Comparing the results of figure 3(a) and figure 6(a), it becomes evident that with a short relevant price history the modified price level calculation of agents forces the system to search an initial high stock price level before it starts oscillating. The initial rise in figure 6(a) is due to the deduction made from the average price ($k_{t-s-1} > k_0$) that pushes

agents to continue buying stock, thus raising the stock price. However, as the parameter *s* is raised and the relevant historic period becomes longer in price level calculations, this initial search phase diminishes and the curve now resembles the result in our first experiment – but with a lower mean stock price due to the deduction of negative stock prices in the agents' price level calculations.

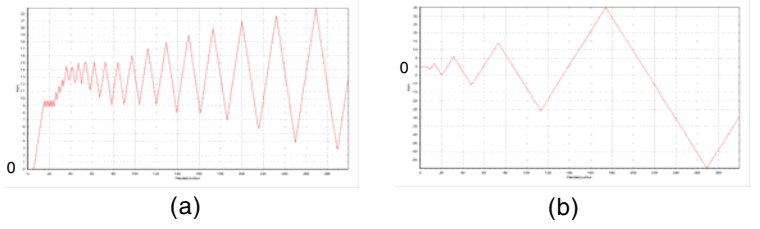


Fig. 6. Results with behavioural agent diversification $d = 0.1$, trading in each period and *s*-value expectation of 10% (a) and 50% (b), standard deviation of *s* is zero. The curves again display the stock price k_t over time during a complete simulation run.

A very significant influence, not seen in experiment 1, comes through the introduction of a standard deviation of *s* (figure 7). With greater diversification of s-values in the agent population, the agents' calculated price level input now varies widely, leading to different price interpretations. The results are substantially reduced amplitude of the stock price movement, shorter oscillation cycles and a lower predictability of the price at the macroscopic level.

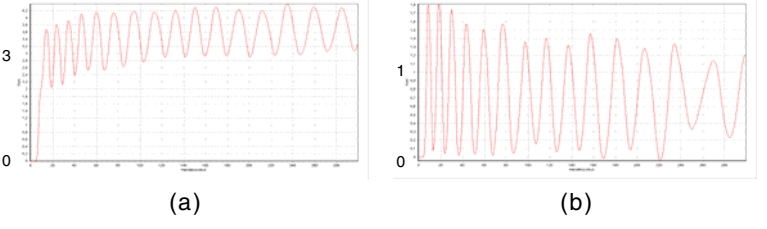


Fig. 7. Results for behavioural agent diversification $d = 0.1$, trading in each period and *s*-value expectation of 10% with a standard deviation of 20% (a) and 30% (b)

4.3 Experiment 3

In this last set of empirical investigations, the influence of a more varied trading frequency is analysed. So far, it was assumed that agents make trading decisions in all periods during the simulation. This is of course not in accordance with real markets, where traders may act more or less frequently, with the extremes of day traders and long-term investors. To emulate such situations we start by introducing an expectation for the random trading frequency *f* that is identical for all agents. This means, all agents continue to trade simultaneously, but not in every period of the simulation. Figure 8 displays the results for this experiment. The curve is less smooth, because of longer intervals without trading, followed by trading periods where the stock price is

abruptly corrected. This is particularly pronounced at the turning points. However, the oscillation of the stock price is less distinctive. The averaging price level calculation of the agents combined with the periods without trading now leads to a stretching of the price oscillation pattern.

Fig. 8. Results for behavioural agent diversification d = 0.3 , trading frequency of 20% with a standard deviation of zero, an s-value expectation of 30% with a standard deviation of zero. The price level calculation is as in section 4.2.

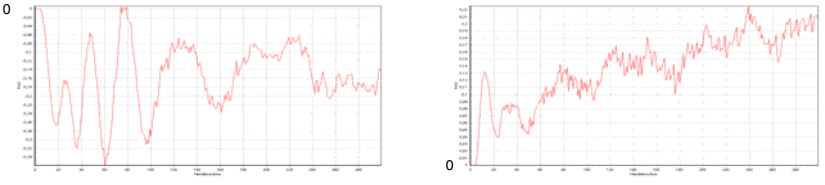


Fig. 9. Results for behavioural agent diversification d = 0.5 (high), a trading frequency of 0% with a standard deviation of 10%, an s-value expectation of 10% with a standard deviation of 30% (a) and 40% (b). The price level calculation is as in section 4.2.

The experiments so far have shown that with the assumption of regular trading it is possible to isolate and interpret the influence of individual model parameters on the macroscopic level. The final simulation serves to demonstrate the effects of more irregular trading, combined with a large behavioural diversity (different market assessments) within the population of agents, when the length s of historic periods used in the price level calculation by the agents is different (figure 9). Stock price now displays a high volatility and resembles real-world stock price patterns. However, the resulting graphs of similar experiments are so different that it seems impossible to draw definite conclusions about the influence of s on the macroscopic level. The interactions of system parameters become too complex to analyse and stochastic influence is visible in the system behaviour.

5 Conclusion and Future Research

The main objective of this paper was a better understanding of the relationship between certain behavioural parameters of the participants of an artificial stock market and the emergent macro-level stock price patterns created through the trading decisions of individual agents. The experiments are certainly preliminary but nevertheless some useful lessons can be learned from the simulations.

First, regular oscillations and complex stock price patterns can be created bottom-up without the necessity of a mathematical top-down model of the simulated market. Moreover, exogenous (economic) shocks to the system are not required to change the direction of the stock price. Nor is it required that agents can communicate directly or use a central coordination instance to achieve aligned behaviour. Focusing on individual traders allows for directly implementing and testing assumptions about the influence of decision parameters and agent behaviour on the simulation.

Second, the trading rules of market participants may be captured with only a few rules using the analogy of technical fuzzy control applications where crisp input combined with a simple model of human knowledge is sufficient to create robust system behaviour. By changing the geometry of fuzzy sets, behavioural variation can be introduced in otherwise identical agents. Thus, we have a straightforward way of modelling some elementary aspects of the psychology of trading behaviour.

Third, seasonal price patterns occur in our simulation just because of price speculations by the individual agents. This would suggest that in real markets oscillations can occur, even if traders ignore all fundamental data. Thus, it does not seem mandatory to refer to interest rates, overall economic situation or exchange ratios – all commonly used to explain trading patterns. This does not mean that fundamental economic data has no influence on individual trading. However, this influence may be overestimated, particularly when it comes to non-professional traders.

Fourth, averaging historic prices in making a trading decision is a fundamental reason for dynamic stock prices, as is behavioural variety amongst traders. A low diversity among traders and similar appreciation of price history suggests regular and very pronounced oscillations of the stock price while greater behavioural variation and a varied appreciation of price history should create volatile and complex price patterns through reinforcement. Thus, stock price forecasting appears to be a hopeless task, even if one could assume *no* change in fundamental data or exogenous shock.

The research outlined here may be extended in various directions. For instance, in our model the stock price is determined in a simplified way that could be improved to more strongly resemble the pricing mechanism of an actual stock exchange. This would include the introduction of a central market maker. The currently small rule base of trader agents could be extended to integrate more inputs or decision variables. Moreover, the rule bases of agents could be different. Evolving trader rules through learning and adaption to different market situations seems to be another interesting extension. Traders might adjust their rule base to maximize personal profit. This could result in a selection mechanism, allowing more successful traders to reinvest their profits while others would have to leave the virtual market. The question which rules and parameter values lead to the best individual long term profit should be addressed in future research. Finally, it would be interesting to simulate exogenous shocks to the stock market system and analyse their effects.

Related current research [19] in our department addresses emergence issues associated with social influence within organisations. Here, we employ a simulation of a large group of agents that are structured in neighbourhoods. Agents follow simple behavioural models that were derived from empirical research. Again, complex macroscopic effects arise from a multitude of locally interacting agents. This points to the necessity of further investigating the micro-macro dependencies in socio-economic systems in particular and complex evolutionary systems in general.

References

1. Uhlig, H.: Finanzmarktanalyse. Vahlen, München (1999)
2. Binswanger, M.: Stock Markets, Speculative Bubbles and Economic Growth. Elgar, Cheltenham (1999)
3. Dette, G.: Kursbildung am deutschen Aktienmarkt. DUV, Wiesbaden (1998)
4. Kaplan, I.: Estimating the Hurst Exponent, `http://www.bearcave.com/misl/misl_tech/wavelets/hurst/index.html` (September 24, 2006)
5. Epstein, J.M., Axtell, R.: Growing Artificial Societies. Random House, London (1996)
6. Kennedy, J., Eberhart, R.C.: Swarm Intelligence. Morgan Kaufman, San Francisco (2001)
7. Bonabeau, E., Dorigo, M., Theraulaz, G.: Swarm Intelligence. Oxford Univ. Press, Oxford (1999)
8. Holland, J.H.: Emergence. From Chaos to Order. Oxford University Press, Oxford (2000)
9. Stephan, A.: Emergenz, 2nd edn. Mentis, Paderborn (2005)
10. Schleis, K.: Börsenpsychologie und Aktienkursprognose. Fortuna, Zürich (1993)
11. Nauck, D., Kruse, R.: Fuzzy-Systeme und Soft Computing. In: Biethahn, J., et al. (eds.) Fuzzy Set Theorie in betriebswirtschaftlichen Anwendungen, pp. 3–21. Vahlen, München (1997)
12. Zimmermann, H.-J.: Fuzzy Set Theory – and Applications, 4th edn. Kluwer, Boston (2001)
13. Sivanandam, S.N., Sumathi, S., Deepa, N.: Introduction to Fuzzy Logic using MATLAB. Springer, Berlin (2006)
14. Tesfatsion, L. (ed.): Special Issue on ACE. Computational Economics, 18, 1 (2001)
15. Loistl, O.: Kapitalmarkttheorie, 3rd edn. Oldenbourg, München (1994)
16. Hommes, C.: Heterogeneous Agent Models in Economics and Finance. In: Tesfatsion, L., Judd, K.L. (eds.) Handbook of Computational Economics, ch. 23, vol. 2. North-Holland, Amsterdam (2006)
17. LeBaron, B.: Agent-based Computational Finance. In: Tesfatsion, L., Judd, K.L. (eds.). Handbook of Computational Economics, vol. 2, ch. 24. North-Holland, Amsterdam (2006)
18. Samanidou, D., Zschischang, E., Stauffer, D., Lux, T.: Agent-based Models of Financial Markets. Reports on Progress in Physics 70, 409–450 (2007)
19. Nissen, V., Saft, D.: Social Emergence in Organisational Contexts: Benefits from Multi-Agent Simulations. Agent-Directed-Simulation Conference (ADS) (2010) (submitted)

A New Neural Network Based Customer Profiling Methodology for Churn Prediction

Ashutosh Tiwari, John Hadden, and Chris Turner

Decision Engineering Centre, School of Applied Sciences, Cranfield University, Bedfordshire, UK
{a.tiwari,c.j.turner}@cranfield.ac.uk

Abstract. Increasing market saturation has led companies to try and identify those customers at highest risk of churning. The practice of customer churn prediction addresses this need. This paper details a novel approach and framework for customer churn prediction utilising a Neural Network (NN) approach. The methodology for customer churn prediction describes a predictive approach for the identification of customers who are most likely to churn in the future. This is a departure from current research into customer churn which tries to predict which customers are most likely to instantaneously churn. A real life case study from industry is presented here to illustrate this approach in practice. Future research will include the enhancement of this approach for more accurate modelling of collective systems.

Keywords: Customer Churn, Churn Prediction Methodology, Customer Profiling, Classification, Neural Network.

1 Introduction

For companies operating in mature markets the acquisition of new customers is a difficult task. It has been reported that the acquisition of new customers can be over ten times more costly to a business than retaining existing customers. This is largely because in saturated markets, the acquisition of new customers often involves enticing customers away from competitors through offers of expensive special deals [1]. Facing a market at or near saturation point a company will soon recognise that its greatest asset is its existing customer base. Holding onto existing customers is not an undemanding procedure; a company must understand its customers and their needs. A route that many organisations have chosen to take involves the use of Customer Relationship Management products to boost customer retention and increase selling opportunities to the existing customer base. Customer retention addresses the issue of customer churn, where churn describes the turnover of customers, and churn management describes the efforts a company makes to identify and control the problem of customer churn [2].

There are several modelling techniques available that can aid in the prediction of customer churn. The most common techniques have been identified from literature as:

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 358–369, 2010.

- Classification and regression trees (CART)
- Logistic regression models (LRM)
- Artificial Neural Networks (NN)

Other statistical and classification methods may also apply to the problem domain, however they have either not been widely explored or they have failed to provide satisfactory results [3]. CART (also known as recursive partitioning regression) is a popular classification technique used for predicting events. The work of Bloemer et al. [4], who detail a classification technique for at risk customers, provides further information on this technique. Logistic regression model (LRM) is an extension of multiple regressions. It provides an output that is in the form of a probability between the values 0 and 1 [5]. Related work in this area is limited to authors such as Mihelis et al. [6] who use such regression techniques for the prediction of customer satisfaction. Artificial Neural Networks (NN) consist of basic elements known as 'neurons'. These neurons consist of three main components: (i) weight, (ii) bias and (iii) activation function. Each neuron receives an input on which it applies a weight value. This weight holds the key to the NN's overall performance because it provides the strength of the connection to the specific input.

Work relating to customer relationship management using NNs has been undertaken by Rygielski [7].Experiments using each of the above mentioned predictive techniques have shown that predictive models alone do not provide a strong enough churn accuracy to make them directly applicable for the capture of future customer churn [8]. To perform churn analysis the predictor variables have to be of sufficient quality. If the predictive model is unable to converge with the data the output predictions will be inaccurate. An examination of literature in this area by the authors reveals that there is only a minimal amount of work in the area of advance churn prediction. In the best cases churn is predicted a maximum of one month ahead. With limited specialist retention staff available to a company, this may be insufficient time for the successful deployment of a retention campaign. A methodology capable of providing a significantly greater time between event and occurrence is therefore required if future customer churn is to be predicted with any accuracy. Literature has also suggested that researchers typically target high churn capture from their models. There has been a lack of documentation that targets the control of misclassification. Misclassifying non-churn as churn add to the numbers that need contacting by the retention department and as customers who never intended to churn are being contacted with expensive retention offers, real churners are left to defect. As mentioned in the previous section demographic, usage and billing data are the most convenient sources for use in predicting customer churn. However, due regulations in place in the case studies industry these sources cannot be used. Instead data collected on repairs and complaints will be used as a basis for this research. Repairs and complaints are common in a huge variety of sectors whereas usage data tends to be industry specific. In many respects the customer churn approach outlined in this paper models the collective behaviour of customers.

2 Customer Profiling Methodology

Current research has concentrated on predicting customer churn as it occurs (i.e. predicting customer churn for a month based on that month's data). The authors' goal is to determine if a NN could predict churn in the future by offering input data from one month to predict the target churn for the following month. However, the results from experiments using this method were poor and an alternative approach was sought. No previous research could be identified for prediction of future churn so the aim was to use the churn index values that had been determined for each customer in this task. From initial experimentation at this stage it was found that the NN provided the customer's propensity to churn on a monthly basis. A theory emerged that customers with similar propensity measures over a set period of time would also display similar characteristics with regards to how long it takes them to terminate their contract. This lead to the development of a customer profile based methodology. By analysing churn indices a number of profile classes could be constructed to categorise different customer types. Clustering was used to produce these classes known as master profiles.

A description of the proposed methodology is as follows:

- **Prepare the data**
  Ensure the data is numerical, and has no missing or incompatible values and take a time sequence of customer data and split the data by customer, by month.
- **Determine the most suitable for creating the NN model**
  One month of data is required for training the NN. The training set should contain as many churners as possible so an analysis of the available data should be performed in order to determine which month contains the highest churn. This month should be used as the basis for creating the training dataset. Based on the total number of churners in the chosen training month randomly eliminate non-churners from the training set to create a 20:80 churn/non-churn ratio.
- **Create an NN suitable for generating a loyalty index**
  Using the training dataset create 3 NNs (1 neuron, 1 layer), (3 neuron, 2 layers), and (6 neuron, 4 layer). It may be necessary to continue these experiments increasing the number of neurons in each layer? By applying each of the NN architectures to the full month that the training set was originally based on, and then comparing the predicted results against the actual churn data, it is possible to determine which NN architecture has converged best. The NN displaying the best convergence should be used for generating churn index values for all other available months.
- **Generate churn index values**
  Using the best NN, generate churn index values for each individual month for each customer. Compile a database containing all churn indices for each month and all churn information.

- **Apply customer profiling methodology**
  Analyse churn indices to establish master profile classes and customer classification into the determined master profile classes.
- **Identify the high and low risk profile clusters**
  By determining how many of the customers contained within each profile cluster have actually churned it is possible to rate each cluster into high-risk and low-risk churn groups.
- **Determine churn capture accuracy**
  Comparing the high-risk profile clusters with future churn data provides a determination of how many future churners have been captured from the resulting methodology. The profiles that have been determined to hold the highest portion of future churn are classified as high risk clusters. The profiles that have small or zero future churn capture classified as low risk clusters. The time frame for the data being analysed is shifted forward. In business the time frame should move on a monthly basis; however for the research it will move forward 3 months to minimise the risk of duplicate capture. This risk would not be a problem in industry as once a customer had churned they would be automatically be removed from the dataset being analysed. The high risk profiles can then be used as future churn predictors and all customers being assigned those profiles classified as churners.
- **Achieve the maximum possible future prediction**
  The profiling methodology has proven to be capable of predicting churn in the future with the ability of matching customers to master profile clusters to enable early classification, increasing time between classification and the actual churn event. The customer profiling methodology uses several months of data to determine customer churn rather than just 1 month as commonly seen in research. Because of this time window a system could easily be implemented in the form of a continuously moving time window capable of classifying customers to master profiles and flagging churn in advance.
- **Base the framework on data that is available across multiple service sectors and accessible for analysis by any business regardless of size**
  Predictions have been based on customer repairs and complaints data. The benefits of using this type of data source are that it is available for use by any company regardless of the monopoly status and it has proved to be a good source for basing accurate future predictions. Churn connected to repairs and complaints is strategic to the specific business. It is the identification of customers who are contemplating defecting because they are not happy with their service so the business is responsible for their dissatisfaction.
- **Minimise the total number of misclassifications from the predictions to reduce retention costs to the business**
  It has been demonstrated that a lot of thought has gone into how misclassification rates can be improved. The customer profiling methodology achieves this task by eliminating customers who fall into weaker churn categories.

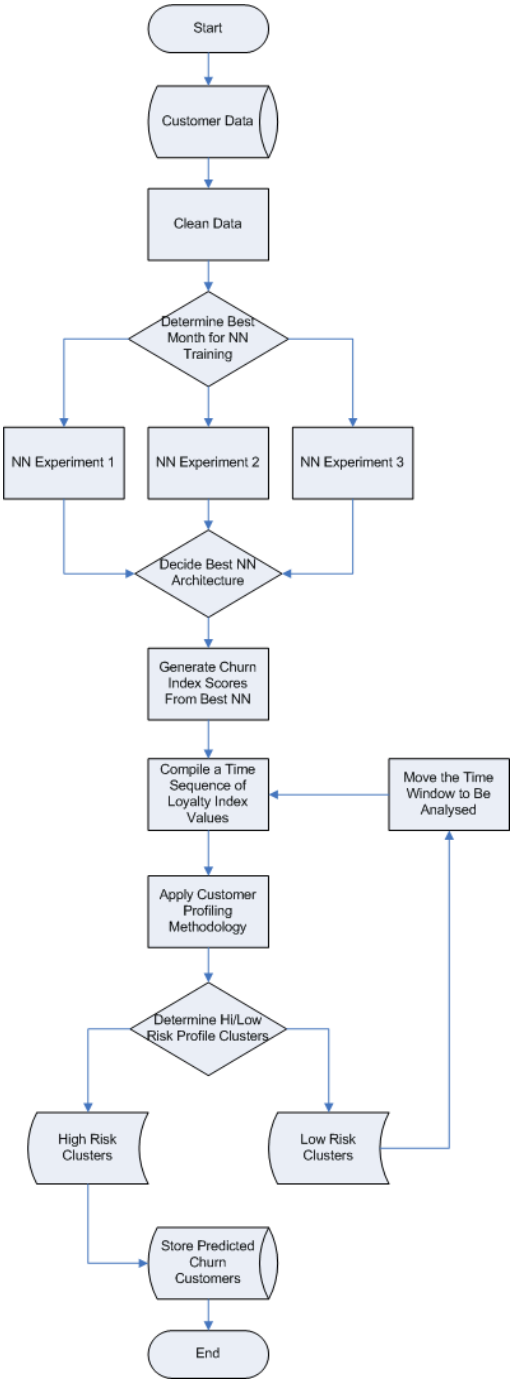


Fig. 1. Customer profiling methodology flow chart

The methodology has been realised in the outline provided in Fig. 1. The key stages to note from Fig. 1 are:

- Decide best month for NN training - One month of data is required for training the NN
- Decide best NN architecture for generating a loyalty index – The loyalty index for a customer is a measure of their comparative loyalty to the company. Three alternative NN architectures are evaluated for this stage
- Generate churn index scores – The churn index indicates a customer's potential to churn. Churn index values are generated for each individual month for each customer. A churn index database is complied out of the results
- Apply Customer profiling methodology - Analyse churn indices to establish master profile classes and customer classification into the determined master profile classes
- Identify high and low risk profile clusters - Analyse churn indices to establish master profile classes and customer classification into the determined master profile classes
- Determine churn capture accuracy - Comparing the high-risk profile clusters with future churn data provides a determination of how many future churners have been captured from the resulting methodology

3 Customer Profiling Case Study

A case study, based on real industry data, was used as further validation of the NN customer churn approach. The data set had the following characteristics:

- 35 variables
- 8408 Customers
- 13 Months of data
- 29:71 Churn\Non-Churn
- 13 Months Containing Churn Activity

To ensure that the most accurate NN architecture is constructed for the generation of a customer churn index several experiments have been performed for the case study using various NN configurations. The first NN experiment used a simple single layer single neuron NN as keeping the complexity of the architecture to a minimum decreases the analysis time. The second NN experiment had a more complex architecture to that of experiment 1 containing 2 hidden layers, each containing 3 neurons each. The third NN experiment involved a large NN. An NN was constructed with four hidden layers and seven neurons per layer. The third NN was much larger than the previous two. This experiment was performed to establish if the complex problem of determining a customer churn rate required a large NN.

3.1 NN Experiment Results

The results obtained from the final NN experiment were very similar to those results of the first single layer single neuron network. The only significant difference between

the results was a decrease in the total number of non-churn misclassifications from the four layer six neuron network, however there are over 2.5 times more non-churn misclassifications generated by NN 3 over NN 2. So that an accurate comparison of the results for all three experiments can be achieved the churn and non-churn accuracies for each experiment were converted to a percentage and recorded in Table 1:

Table 1. NN prediction accuracy result

Activation Function	Churn Capture Accuracy	Non-Churn Capture Accuracy	Total Accuracy
NN1	76.50%	94.00%	93.40%
NN2	65.50%	98.40%	97.40%
NN3	73.80%	96.00%	95.30%

It can be observed from Table 1, NN1 experiment achieved a total prediction accuracy of 93.4%. The total prediction accuracy has been calculated by adding the correct number of classified non-churn with the correct number of classified churn, dividing the number by the total dataset size of 8409 and multiplying by 100. NN2 achieved a 97.4% total accuracy and NN3 achieved a 95.3% total accuracy. From this information it is clear that the NN2 configuration has provided the best overall results for classifying the case study dataset.

3.2 Generating Churn Index Values

The results obtained from NN experiment 2 shown in Fig. 2 are appropriate for generating churn index values because they provide a significant number of actual churn matches with a decrease in non-churn misclassifications over those generated from NN 1 and NN 3. The 2nd NN configuration is used to generate churn index values for each customer over each month of the available historical dataset for analysis by the customer profiling methodology. Once the churn index values for each month are generated they are exported out of Matlab and inserted into MS Excel. The first Excel column is the customer ID number, column 2 is the churn index values for April 04, Column 3 May 04, etc. After all the months are inserted, the churn column is added to the worksheet. This column stores as a numerical indicator depending on the month churn occurred. E.g. If the first month of data in the time sequence is April 04 then the corresponding churners for April 04 are stored as the integer '1'. May 04 churners are given the integer '2', June 4 the integer '3' etc. This is because the profiling methodology attempts to identify a pattern of how long it takes customers to churn after their loyalty index values fall below a pre-defined churn threshold. If the churn index value falls below the churn threshold in month 2 and actual churn occurs in month 4 then that particular customer took 2 months to churn. If all customers belonging to a profile take 2 months to churn we have determined that all customers being matched to that profile should also theoretically take 2 months to churn.

ID	Apr-04	May-04	Jun-04	Jul-04	Aug-04	Sep-04	Oct-04
1	0.0000	0.0027	0.9961	0.0156	0.0020	0.0004	0.0000

Fig. 2. Churn index values

An example of the required customer churn index values that are used for analysis by the churn profiling software can be seen in Fig. 2.

3.3 Applying a Customer Profiling Methodology

The churn index values such as the ones shown in Fig. 2 are presented to the churn profiling software. The profiling software methodology performs its analysis in the following sequence:

- Convert the churn index values to loyalty index values using the formula *Loyalty index = 1 – churn index*
- Assess the loyalty index values to see if their has been fluctuating activity for the customer
- Check to see if loyalty profiles already exists for determined loyalty time series pattern.
- If the profile exists, assign the customer that profile.
- If the profile does not exist check to see if the customers loyalty value at any point falls below a given churn threshold (The value 0.3 has been defined as a default value because this value provided best accuracy during the initial methodology experiments).
- If the loyalty index value has fallen below the churn threshold check to see if the customer is recorded as an actual churner.
- If the customer has been recorded as an actual churner, add the profile for that customer as a future master profile.
- If the customer is not an actual churner or the customers loyalty index value has not fallen below the churn threshold then do nothing.

An example result for master profile 11 is shown below in Fig. 3. This profile shows an initial raise in the customer's loyalty index which then levels off for one month before a major drop that brings the loyalty index below the churn threshold. Only 9 customers fell into this profile, out of which a total of 7 customers actually churned and 5 of these customers churned in the three month future period.

As shown from the example master profile in Fig. 3 the profile separates into two sections. A line chart at the top of the master profile display window provides a visualisation of the customer's loyalty index pattern. In the case of master profile 11 Fig. 3 shows an initial raise in the customer's loyalty index which remains static for 1 month before a major decline in loyalty value that brings the customer's loyalty level below the churn threshold. Similarly master profile 38, shown in Fig. 4, begins with an initial decline in customer loyalty although this decline is not significant enough to lead to customer churn. A final major event in month 4 is significant enough to lead to customer churn. The bar chart at the bottom of the window illustrates approximately how long it took the customers who churned within the analysis period to churn after their loyalty index values fell below the churn threshold. This approximation is a

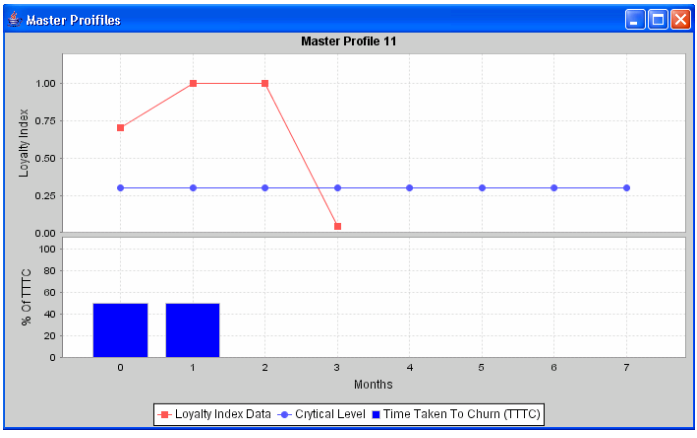


Fig. 3. First most significant profile for future churn capture

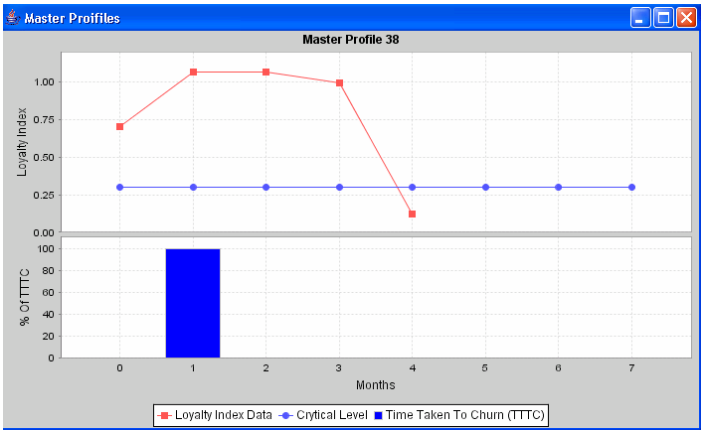


Fig. 4. Third most significant profile for future churn capture

calculation based on all customers belonging to that master profile cluster who have actually churned. It is the average time taken for each customer to churn after their loyalty index value fell below the specified churn threshold This chart shows that for the case of master profile 11 50% of the customers churned within the same month as the event that caused the major fall in customer loyalty and 50% churned 1 month after the significant fall in customer loyalty. Only 2 customers churned within the analysis period for master profile cluster 11.

3.4 Determining Future Churn Capture Accuracy

The case study dataset contains 13 months of data. The first 7 months have provided the input to the profiling methodology, while the subsequent 3 months have been used for classification of future churn accuracy for each of the master profile cluster. If, out of all the master profiles generated from this dataset, the master profiles categorised

as strong churn classifiers (such as master profile 11 shown in Fig. 4) are aggregated, the future churn captured from these profiles total 189 from 758 customers who actually churn three months future of the analysis period. This is 25% of all churn over the future period. The most important aspect of the research though is the enhancement of the hit ratio, as the hit ratio in essence defines the strength of the predictive methodology. The overall hit ratio achieved from the test phase is 0.64. This means for every 1.5 customer's contacted 1 customer will be a future churner. 10 months of data has been required to generate the customer profiling predictive model and the dataset contains a total of 13 months of data. The analysis window is moved forward 4 months to fully test the predictive accuracy of eight master profiles that have been identified as being the best for future prediction using months August to February as inputs for generating profiles for the prediction of the final 2 months of the dataset, March and April (two profiles were excluded from this experiment due to their low membership). The actual future churn capture for the dataset is displayed using the confusion matrix in Fig. 5.

	Estimated Labels		
True Labels	0	1	Totals
0	7381	526	7907
1	345	156	501
Totals	7726	682	8408

Fig. 5. Initial future predictions from the case study dataset

As can be seen from Fig. 5 the initial future predictions have caught 31% of future churn. The results as they are have achieved a hit ratio of 0.22 so basically from every four predictions, one is an actual churner.

4 Discussion of Results

For easy analysis the results obtained from all three methodologies have been compiled into the bar chart shown in Fig. 6. It is evident from the results for each methodology shown in Fig. 6 that the customer profiling methodology has outperformed the NN proposed by Hu [9] and the one proposed by Hwang et al. [10]. Both of these alternative methodologies have similar results for both churn prediction and corresponding non-churn misclassifications. The customer profiling methodology has captured significantly more churners. The misclassifications for the customer profiling methodology are much lower than the other two methodologies and a large proportion of total predictions did actually churn. It should be noted that the average monthly churn has been used for the customer profiling methodology and so has the average monthly non-churn misclassification.

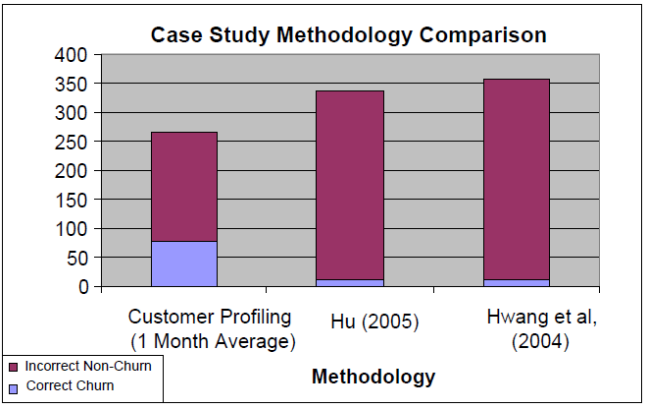


Fig. 6. Comparison of methodologies for case study

The total churn capture for each methodology does not define the power of that methodology as prediction accuracy is directly related to the quality of the input data. The power of the model is defined by the hit ratio (the total number of predictions divided by the total number of correct classifications). The hit ratio provides an accurate measure of how well the model has determined predictions. The data used for analysis is not of very good quality which is apparent from the actual churn capture. The fact that the data is of poor quality is reflected through the Hu [9] and Hwang et al. [10] models. These models use general classification techniques and the results would show much stronger if the data was of better quality. The data does however; provide a suitable measure for model performance as the prediction accuracy measured by hit ratio does not require perfect data for churn prediction. Regardless of data quality, the profiling methodology has achieved a hit ration of 2.4 using monthly averages, which is over ten times better than either the Hu [9] results or Hwang et al. [10] results. The validation experiments performed on the case study data have determined that the customer profiling methodology has considerably outperformed the other techniques.

5 Conclusions

This paper has detailed a novel approach and framework for customer churn prediction utilising a Neural Network (NN) approach. A methodology for customer churn prediction and the identification of customers who are most likely to churn in the future has been presented. This is a departure for current research into customer churn which tries to instantaneously predict which customers are most likely to churn. A real life case study from industry has been presented here to illustrate this approach in practice. The results obtained from the case study show promise in the prediction of future customer churn. This research can be located within the framework of a collective evolutionary system. Indeed the collective behaviour of customers can be understood at a greater level of detail using the approach outlined in this paper. The accuracy of the learning stage of the NN approach, detailed in this paper, could be

enhanced by its combination with an evolutionary optimisation technique such as genetic algorithms. Further to this concept an intelligent feedback loop may be built into a customer churn system to automatically respond to groups of users likely to churn with an appropriate offer or combination of offers. The modelling of collective systems could be possible with such an enhanced system outlined here. Future research could include the further study of customer behaviour, web based communication systems and even stock markets.

References

1. Seo, D., Ranganathan, C., Babad, Y.: Two-Level Model of Customer Retention in the US Mobile Telecommunications Service Market. Telecommunications Policy 32(3-4), 182–196 (2008)
2. Hung, S., Yen, D.C., Wang, H.: Applying Data Mining to Telecom Churn Management. Expert Systems with Applications 31, 515–524 (2006)
3. Coussement, K., Van Den Poel, D.: Churn Prediction in Subscription Services: An Application of Support Vector Machines While Comparing Two Parameter-Selection Techniques. Expert Systems with Applications 34, 313–327 (2008)
4. Bloemer, J., et al.: Comparing Complete and Partial Classification for Identifying Customers at Risk. International Journal of Research in Marketing 20, 117–131 (2002)
5. Nefeslioglu, H.A., Gokceoglu, C., Sonmez, H.: An Assessment on the Use of Logistic Regression and Artificial Neural Networks With Different Sampling Strategies for the Preparation of Landslide Susceptibility Maps. Engineering Geology 97, 97–171 (2008)
6. Mihelis, G., et al.: Customer Satisfaction Measurement in the Private Bank Sector. European Journal of Operational Research 130, 347–360 (2001)
7. Rygielski, C., Wang, C.J., Yen, D.C.: Data Mining Techniques for Customer Relationship Management. Technology in Society 24, 483–502 (2002)
8. Hadden, J.: A Customer Profiling Methodology for Churn Prediction. PhD Thesis, Cranfield University, UK (2008)
9. Hu, X.: A Data Mining Approach for Retailing Bank Customer Attrition Analysis. Applied Intelligence 22, 47–60 (2005)
10. Hwang, H., Jung, T., Suh, E.: An LTV Model and Customer Segmentation Based on Customer Value: A Case Study on the Wireless Telecommunications Industry. Expert systems with applications 26, 181–188 (2004)

Phonological Recoding in the Second Language Processing*

Chang H. Lee[2], Kyungill Kim[1,**], and HeuiSeok Lim[3]

[1] Department of Psychology, Ajou University, Korea
kyungilkim@ajou.ac.kr
[2] Department of Psychology, Seogang University, Korea
chleehoan@seongang.ac.kr
[3] Depart of Computer Science Education, Korea University, Korea
limhseok@korea.ac.kr

Abstract. A phonological priming task was conducted in order to determine the presence of second language phonological recoding. Eighteen Koreans who had acquired English after a critical language learning period participated in the experiment. Compared with controls, the phonological condition (e.g., TOWED -> toad) was more advantageous in processing the target in the priming task than the orthographic condition (e.g., TOLD -> toad). This result indicates that second languages are learned and processed phonologically rather than orthographically.

1 Introduction

The role of phonological information in English second language processing has important theoretical and practical implications. Many studies have shown that English second readers use a phonological code that was transformed from orthographic letters in word recognition [3] [6] [7]. These studies commonly showed that phonological awareness, the ability to manipulate phonological units in a word, is significantly correlated with second language development. Although many previous studies have shown that phonological information is used in English second language processing, they have not focused on the early stage of word processing. Thus, it remains unconfirmed whether a word is phonologically recoded before accessing the lexicon, i.e., the entry of word representation.

Use of the fast priming task is one of the best ways to tackle the early stage of word processing (e.g., Lukatela, Eaton, Lee, Carello, & Turvey, 2002). In a forward priming task, two stimuli are presented serially with the latter being the target to name, or conduct some designated behavior, while the former is called

* This research was supported by the Original Technology Research Program for Brain Science through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2009-0093899).

** Corresponding author.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 370–375, 2010.

the prime. The degrees of overlap for phonological information between the prime and target were manipulated in order to investigate the role of phonological information. It has been found that providing more phonological overlap between the prime and target (e.g., TOWED [prime] -> toad against its control) was more advantageous than providing deficient phonological overlap between them (e.g., TOLD -> toad). Many studies on native language processing have demonstrated the necessary role of phonological information using the priming task.

This brief study employed this fast priming task to confirm the phonological recoding in second language processing by using English second language readers. The stimuli were obtained from Lukatela et al.'s (2002) seminal priming study that showed phonological recoding in mother language processing. This study used their stimuli and experimental design to investigate the processing in English second language processing.

The seminal study that showed phonological processing for the second language is Brysbaert, Van Dyck, and Van de Poel (1999)'s study. Their study showed that the phonological prime of Dutch (mother language) can facilitate the processing of the second language, English in this study. This indicates that the phonological form of English can be accessed fast, meaning the possibility of phonological processing of the second language. Subsequently, Wijnendaele and Brysbaert (2002) showed that the phonological prime of French (the second language in this study) can facilitate the processing of mother language, Dutch in this study. This finding further strengthen the argument that the phonological form of the second language can be activated automatically and fast.

2 Experiment

Although Brysbaert, Van Dyck, and Van de Poel (1999) used interligual priming to investigate the phonological processes for mother language and the second language, it is necessary to conduct a study with only second language to know whether phonological form can be activated without the presence of the mother language. Among many studies that used phonological priming with one language, Lukatela and Turvey (1994)'s study was the seminal study to prove the phonological recoding of mother language.

Lukatela and Turvey's (1994) compared the phonological priming (e.g., TOWED - toad) and its control priming (e.g., PLASM - toad), and the orthographic priming (e.g., TOLD - toad) and its control priming (e.g., GIVE - toad). They found that the phonological priming produced more facilitation in naming the target than did the orthographic priming.

The participants in this study were Korean college students who had learned English as a second language from middle school. They didn't have a native language processing proficiency, but their English reading and writing ability was advanced. They were therefore desirable subjects to investigate the role of phonological information in English second language processing.

3 Methods

3.1 Participants

Eighteen college students enrolled in a social science class participated in the Eexperiments 1. None of the participants had ever lived abroad and they had only learned English from middle school. Their self-reported TOEFL scores ranged from 520 to 600. Their average age was 22.4, and 9 male and 9 female students participated in this experiment as a partial fulfillment of the course credits.

3.2 Materials and Procedures

Most of the stimuli to manipulate the phonological information between the prime and target were selected from Lukatela and Turvey's (1994) study. The primes and targets were categorized into the following four lists: list 1 was composed of 88 phonologically overlapped, prime-target pairs (e.g., TOWED - toad), list 2 of quasi-homographically related prime-target pairs (e.g., TOLD - toad), and lists 3 and 4 of their respective controls (e.g., PLASM - toad for TOWED - toad; GIVE - toad for TOLD - toad). The control primes were selected as having the same frequency and length as the target, but sharing no identical letter in the same position as the targets. Overall target word frequency was 1115, and the average prime frequency was 1982, 1013, 1954, and 1075, respectively for list 1-4. Thus they were all high frequency words, which are the main focus in word recognition studies. In addition, they are matched in phonological and orthographic conditions for their respective controls.

The participants were asked to name the target. The target stimuli appeared at the center of the computer screen that was refreshed at a rate of 78 Hz with a refresh duration of 12.0 ms. Following Lukatela and Turvey's (1994) study, a four-field priming task (i.e., Mask-Prime-Mask-Target) was used. The presentation and duration of the stimuli were controlled by the DMASTER software, which was developed at Monash University and the University of Arizona by Forster and Forster. The four visual events were presented in the following order: (1) five hash marks for 490.2 ms, (2) a row of capital case primes for 129 ms, (3) a row of ampersands for 90.3 ms, and (4) a lowercase word target for 2000 ms. The duration of the prime was set at approximately 120ms in order to reflect the early stage of word processing. The above presentation order was cycled and the stimuli were located in the same place in the center of the screen.

4 Results

The response latencies less than 250ms and more than 2000ms were treated as outliers; they comprised than 0.7% of all response latencies [11]. The mean latencies and their standard deviations for each condition are shown in Table 1.

A 2×2 within analysis of variance (ANOVA) was performed. One factor was a priming type (priming vs. control), and the other factor was a phonological manipulation type (identical vs. deficient).

Table 1. Mean Lexical Decision Latencies (in Milliseconds) and Error Percentages as a Function of Experimental Presentation Condition

	Phonological			Orthographical		
	Mean	SD	Error	Mean	SD	Error
Primining	620	45	0.5	632	51	0.7
Control	652	49	0.8	636	47	0.9

The effects of the priming type were statistically significant ($F1(1,17) = 40.5.32$, $MSE = 6264.43$, $p < .001$, $F2(1,87) = 11.10$, $MSE = 45807.5$, $p < .01$), but those of the phonological manipulation (i.e., phonological vs. orthographical) were not (all $Fs < 1$). There was also significant interaction between the prime type and phonological manipulation ($F1(1,17) = 13.85$, $MSE = 3682.12$, $p < .01$, $F2(1,87) = 3.81$, $MSE = 14299.12$, $p < .05$).

Error analysis was not conducted because all error rates were below 1% for each participant, thereby invalidating any comparison.

5 Discussion

This study was conducted to determine whether early phonological information intervenes in the processing of second language for Korean English bilinguals. Using the priming task, the results indicated that providing more phonological information between the prime and target increased the performance, thus suggesting that early phonological activation would engage in second language processing.

The characteristics of the mother language may have been transferred to the second language (e.g., Atwill, Blanchard, Gorin, & Burstein, 2007; Hamada & Koda, 2008). In other words, because Korean is also alphabetic and proven to be processed by phonological code, it is quite possible for Koreans to use a similar type of unit in learning and eventually processing foreign language (Kim & Lee, 2004). Further studies are needed in order to confirm this hypothesis.

A related issue in second language phonological processing is the bilingual phonological priming task. As mentioned earlier, mMany bilingual priming studies have shown the significance of L1(mother language)-L2(second language) phonological priming [2] [4] [13]. In other words, providing the same phonological information between the prime and target (L1 for the prime and L2 for the target, or vice versa) was beyond merely providing deficient phonological information. This indirectly suggests that L2 would be also processed phonologically. Although phonological information would be used in English second language processing based on these kinds of study, their methods have serious limitations that prevent any firm conclusions from being made on this issue. Their stimulus presentation was always accompanied by the presentation of the mother language. The presence of the mother language might have elicited phonological

processing as it has been argued that many alphabetic mother languages are processed phonologically. Thus, the current study results based on the use of only L2 words provided better evidence on the L2 phonological process.

The present study has extended the success of the study by Lukatela et al. (2002) in showing the phonological priming for the mother language process. If a mother language is processed phonologically, it will be efficient to learn and process a second language using the same processing mechanism. This leads naturally to the nature of the role played by the orthographic information. The phonological recoding hypothesis for the mother language can also be applied to the second language [12]. Specifically, the orthographic route connecting the visual form of letters to the lexicon will be developed earlier than the phonological route. Nevertheless, the orthographic route is inefficient because of its arbitrary connection between the symbolic letter and meaning. Thus, the phonological route, with its rules for the transformation of letters into phonemic strings, should be used in skilled reading.

References

1. Atwill, K., Blanchard, J., Gorin, J.S., Burstein, K.: Receptive vocabulary and cross-language transfer of phonemic awareness in kindergarten children. Journal of Educational Research 100(6), 336–345 (2007)
2. Brysbaert, M., Van Dyck, G., Van de Poel, M.: Visual word recognition in bilinguals: Evidence from masked phonological priming. Journal of Experimental Psychology-Human Perception and Performance 25(1), 137–148 (1999)
3. Cheung, H.: The role of phonological awareness in mediating between reading and listening to speech. Language and Cognitive Processes 22(1), 130–154 (2007)
4. Gollan, T.H., Forster, K.I., Frost, R.: Translation priming with different scripts: Masked priming with cognates and noncognates in Hebrew-English bilinguals. Journal of Experimental Psychology: Learning, Memory, and Cognition 23(5), 1122–1139 (1997)
5. Hamada, M., Koda, K.: Influence of first language orthographic experience on second language decoding and word learning. Language Learning 58, 1-31 (2008)
6. Harrison, G.L., Krol, L.: Relationship between L1 and L2 word-level reading and phonological processing in adults learning English as a second language. Journal of Research in Reading 30, 379–393 (2007)
7. Jongejan, W., Verhoeven, L., Siegel, L.S.: Predictors of reading and spelling abilities in first- and second-language learners. Journal of Educational Psychology 99, 835–851 (2007)
8. Kim, Y., Lee, C.H.: The role of phonological information in processing monosyllabic Korean words. Korean Journal of Cognitive Science 15, 35–41 (2004)
9. Lukatela, G., Eaton, T., Lee, C.H., Carello, C., Turvey, M.T.: Equal homophonic priming with words and pseudohomophones. Journal of Experimental Psychology-Human Perception and Performance 28(1), 3–21 (2002)
10. Lukatela, G., Turvey, M.T.: Visual lexical access is initially phonological: 1. Evidence from associative priming by words, homophones, and pseudohomophones. Journal of Experimental Psychology: General 123(2), 107–128 (1994)

11. Ulrich, R., Miller, J.: Effects of truncation of reaction time analysis. Journal of Experimental Psychology: General 123, 34–80 (1994)
12. Van Orden, G.C., Goldinger, S.D.: Interdependence of form and function in cognitive systems explains. Journal of Experimental Psychology / Human Perception & Performance 20(6), 1269 (1994)
13. Van Wijnendaele, I., Brysbaert, M.: Visual word recognition in bilinguals: Phonological priming from the second to the first language. Journal of Experimental Psychology-Human Perception and Performance 28(3), 616–627 (2002)

A Personalized CALL System Considering Users Cognitive Abilities

Saebyeok Lee, WonGye Lee, Hyeon-Cheol Kim,
Soon-Young Jung, and HeuiSeok Lim

Depart of Computer Science Education, Korea University, Korea
limhseok@korea.ac.kr

Abstract. This paper proposes a Computer Assisted Language Learning(CALL) system, the English Brain Enhancement System, in which is applied the brain scientific principles of human language processing for effective English learning. It is designed to offer adaptive learning based on the cognitive abilities related human language processing. For this, the system has a cognitive diagnosis module which can measure five types of cognitive abilities through three tests. The results of this diagnosis are used to create dynamic learning scenarios for personalized learning services and to evaluate user's performance in the learning module. This system is also designed for users to be able to create learning lists and share it simply with various functions based on open APIs. Additionally, through experiments, it shows that this system help students to learn English effectively as using more internal linguistics memory.

1 Introduction

English learning is very crucial and inevitable for entrance to university and for getting a competitive job in Korea. Most of Korean students start to learn English from their early kindergarten. They learn English through private education system as well as public education system.

Last decade, in Korea, the private education cost for English learning has grown remarkably. it has increased to more fifteen trillion dollars that reached 65% of the total cost of the private education [1]. It has been found that from middle school to university that Korean students invest 4 hours per day on average to study English This is 1.5 times more than the average time of countries in the OECD [2]. According to ETS [3] statistics, 19% of the total number of applicants for TOFEL [4] are Korean and, in TOFEL scores, Korea is 89th among 147 countries [5]. In other words, the effect of English education in Korea is very low. This inefficiency in English learning is not only a problem in Korea but also in most of non-English-speaking countries, such as Japan, China and Vietnam.

Recently, many teaching strategies and methods for English education have been developed and used. One of common features of these strategies and methods are that English education should be proceeded to be adapted to student's abilities. Another common feature is that students are able to study English steadily anywhere, anytime. Especially, computing education environments named CALL (Computer Assisted Language Learning) show effective results as a education supporting tool, offering services

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 376–384, 2010.

satisfied these features to students. Additionally, according to recent researches on foreign language education, it is reported that brain scientific principles of human language processing, such as verbal span size, working memory and cognitive abilities relating language comprehension and production, strongly influence the foreign language learning [6].

Thus, for more effective English education, students' cognitive abilities related brain scientific principles of human language processing should be considered. There have been few CALL systems considering students' cognition abilities for foreign languages processes.

Therefore, in this paper, we propose a CALL system, English Brain Enhancement System(EBEN). The proposed system is designed to offer English learning adopted to user's cognitive abilities based on brain scientific principles. For this, the system has a cognitive diagnosis module which can measure five types of cognitive abilities with three tests. And this diagnosis results are used to creating dynamic learning scenario for personalized learning services and evaluating various user's performances. This system is also designed for users to be able to create learning lists and share it easily with Google open API [7]and it has been developed based on ajax [8] for usability. This paper is organized as follows. Section 2 introduces various researches related CALL systems and cognitive abilities for foreign language learning. Section 3 presents English Brain Enhancement System in detail. and Section 4 concludes this paper.

2 Related Works

CALL originates from CAI (Computer-Accelerated Instruction) and it means the use of computers for language teaching and learning [9]. The distinct features of CALL are that it offers a powerful self-access facility and, in CALL, learning materials adapt themselves to the requirements of the individual student [10]. The smart.fm [11] is an web-based vocabulary learning system in which these features have been reflected very well lately. And it offers three types of learning that are multiple-choice questions, dictations and games for vocabulary learning. It is also an user-created system in which the users can build up the word listsand share it freely for other users.

On other hand, recently, It is actively investigated that principles of human language processing affect the foreign language learning in brain science domain. Especially, as shown Fig. 1, it is found that native language processing and foreign language processing are different and they have intimate relations with each other. it shows that principles of human language processing should be considered for effective foreign language learning. The Lexia [12] is an English learning program to restore for dyslexia based on principles of human language processing in brain. It offers the diagnosis service to measure the language processing ability in brain and it consists of five learning steps customized by the diagnosis results, such as phoneme distinction, pronunciation, lexical meaning, and understanding of sentence. But it is insufficient to apply English learners in non English-speaking countries directly because it made for native English dyslexia patients.

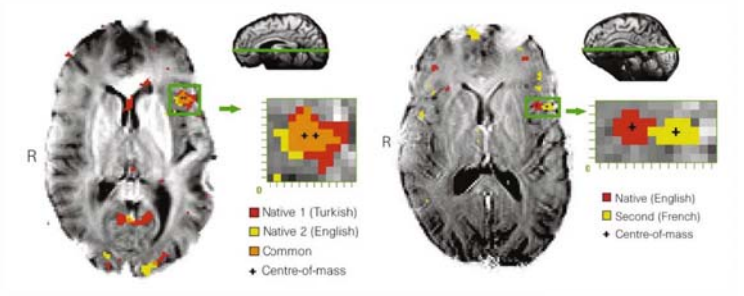


Fig. 1. Difference of Brain Areas of Activation Between Native and Foreign Language Processing [6]

3 The English Brain Enhancement System

3.1 Overall Architecture

As shown in Fig. 2, the proposed system consists of four modules. The first is the cognitive diagnosis module that measures user's cognitive ability-related human language processing and foreign language abilities for personalized learning. And measuring cognitive ability is the size of verbal span and working memory [13]. And Measuring foreign language abilities are listening, reading, writing and producing abilities. The second module determines the learning information used in the learning module based on a user's measured ability. In the second module, several learning information is determined for personalized learning such as the number of words to learn at one time and the number of choices for multiple-choice questions. The third is the learning module where users actually process the learning with personalized learning information. In third part, the evaluation of learning performance is also carried out immediately based on measured foreign language abilities in the first module. The last is the management module for learning word lists. This part is developed based on the web with Ajax [14] and helps the user to be able to create word lists to share conveniently. It also offers several useable functions such as auto-translation, auto-image search and auto-stance search.

3.2 Diagnoses Module

The proposed system carries out following tests for diagnoses of user's cognitive abilities related brain scientific principles and foreign language process abilities. All tests are developed to have pre-tests for instructions.

1. *Verbal Span Test* : This is for measuring the size of a user's memory for foreign language vocabulary and working memory. As shown in Fig. 3, this test is designed to have several levels. Each level means the size of a user's foreign languages vocabulary memory and working memory.
2. *Lexical Decision Task (LDT)* : This is for measuring a user's foreign language processing ability for listening, reading and writing. Each ability is measured by

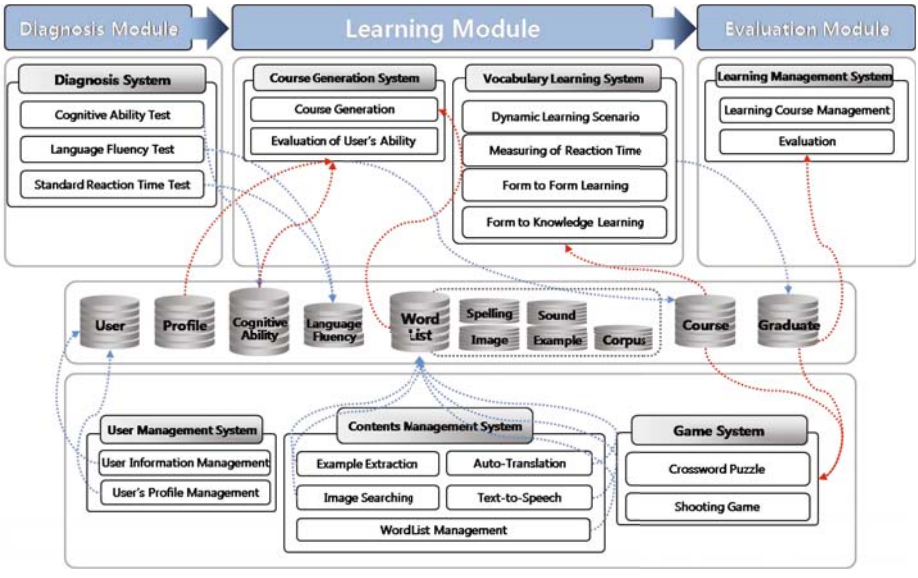


Fig. 2. System Architecture

listening LDT, reading LDT and writing LDT. These LDT tests are designed to measure reaction time when the indicated tasks for each ability are executed as shown in Fig. 4.

3. *Priming Test* : This is for measuring a user's production ability for foreign languages. In other words, it measures how fast a foreign language is able to be applied when a foreign language is required. So, this test can be used to measure speaking ability indirectly. As shown in Fig. 5, this test is also designed to measure reaction time like Lexical Decision Task.
4. *Standard Reaction Time Test* : This is for measuring base reaction times used for immediately evaluating a user performance in the learning module. Immediate evaluation of user performance is carried out by comparing the reaction time taken in learning tasks with measured basis reaction time in this test. Therefore, it is designed to have 11 types of the same learning tasks used in the learning module and to measure the reaction time of these learning tasks as shown in Fig. 6. Additionally, this immediate evaluation is used to create dynamic learning task scenarios in the learning module for personalized learning.

3.3 Personalized Learning Features

The proposed system provides personalized foreign language learning which is based on the diagnostic results of cognitive and foreign language abilities. The personalized learning module exploits several features to make a best-fit learning procedure for a user. The features used in the modules are as follows :

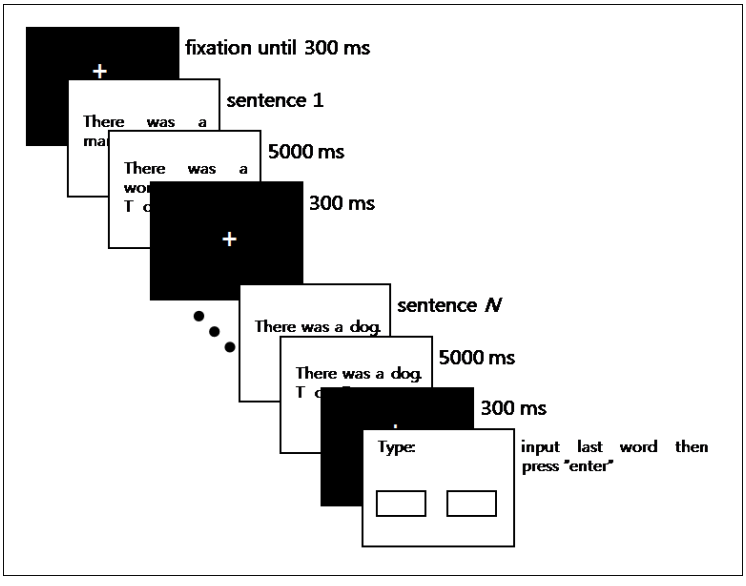


Fig. 3. Verbal Span Test (design and implementation)

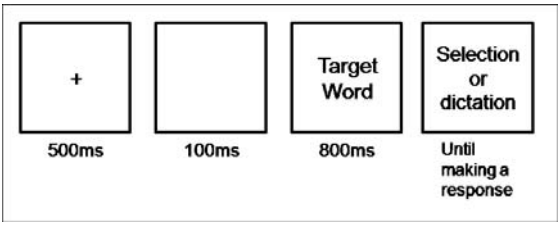


Fig. 4. Lexical Decision Task (LDT) (design and implementation)

- *The number of word to learn at same time* : To maximize each user's memory ability, the number of words that user learns concurrently is determined by Verbal Span test.
- *Test The number of options include in multiple-choice questions* : It means the size of feasible choice sets in the learning module. This is also determined by Verbal Span Test.
- *Word presentation time as word length* : For efficient learning, learning words are presented during a minimum time based on word length.
- *The period of re-learning accord to Ebbinghaus' forgetting curve* : The proposed system offers repetitive learning at 10 minutes, daily and monthly intervals based on Ebbinghaus' forgetting curve.
- *Reacting times in the learning for dynamic learning scenario* : It is explained in the Standard Reacting Time Test in Section 3.2 and 3.4

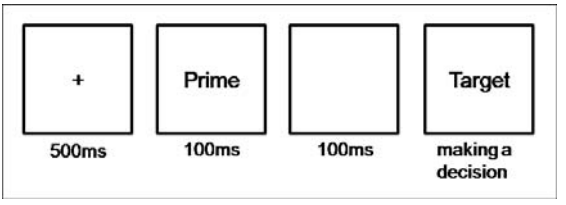


Fig. 5. Primming test (design and implementation)

Fig. 6. Standard Reaction Time Test (design and implementation)

3.4 The Learning Module

The proposed system has two levels of foreign language learning based on brain scientific human language Learning models as shown in Fig. 7. The first level is Form-to-Form learning that is a course to memorize word's information such as spelling and pronuncication without considering meaning. The second level is Form-to-Knowledge learning which is a course to connect word information, memorized in Form-to-Form leaning, with responses of native language and images and stances.

Both Form-to-Form and Form-to-Knowledge learning levels have 15 learning tasks, that a user actually carries out. They consist of spelling, pronunciation, a word response, an image, and a stance with personalized learning information explained in Section 3.3. Follows are learning task and descriptions of Form-to-Form and Form-to-Knowledge learning.

1. *Form-to-Form*: Form-to-Form learning consists of eight learning tasks as shown in Fig. 8. It is divided into two types of leaning forms that are showing and problem-solving. The showing form means that the system shows all information of word with instructions, such as "Listen and speak" or "Repeat the presented word". Then users just carry out the presented instructions. The problem-solving form means that the system shows problems about a word, and then users answer the correct word information.

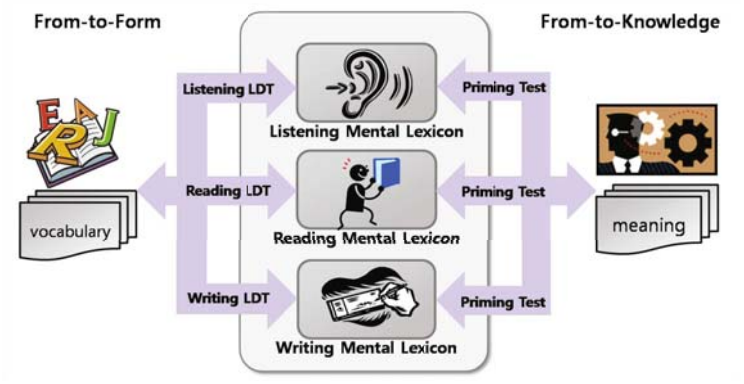


Fig. 7. Brain Scientific Language Process Model

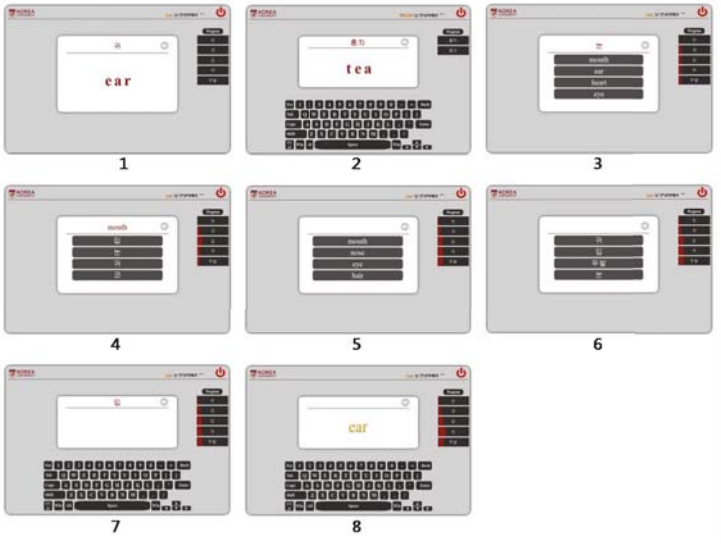


Fig. 8. Form-to-Form Learning Scenes

2. *Form-to-Knowledge*: Form-to-Knowledge learning consists of seven learning scenes as shown in Fig. 9 and it also has two types of learning forms similar to Form-to-Form learning.

In the proposed system, the dynamic learning task scenario which constitutes the sequence of all 15 learning tasks, based on a user's diagnostic information as explained in Section 3.2, is offered for personalized learning. It is designed to determine the next learning task based on user performance which is evaluated immediately at every learning task. Evaluation is based on a user' basic reaction time measured by the Standard Reaction Time Test explain in Section 3.2. The following Listing 1 is the algorithm of the dynamic learning scenario.

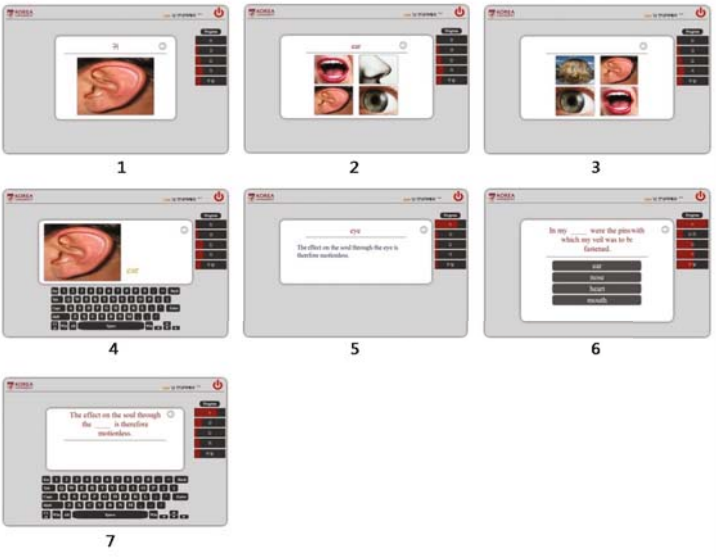


Fig. 9. Form-to-Knowledge Learning Scenes

Algorithm 1. The Algorithm of the Dynamic Learning Scenario

```
1:  procedure DynamicLS(evaluation)
2:      *wordindex = indicate word index in word list array
3:      if evaluation is "Incredible" or "Bad" then
4:          if evaluation is "Bad" then
5:              badCount += 1
6:          end if
7:          if badCount ¿ 3 then
8:              sceneNumber = learningscene
9:          else
10:             sceneNumber = nextscene
11:         end if
12:     else
13:         wordNumber = nextword
14:         sceneNumber = nextscene
15:     end ifreturn sceneNumber, wordNumber
16: end procedure
```

4 Conclusion

In this paper, we proposed a CALL system named English Brain Enhanced Learning, based on brain scientific principles of human language processing. It is a pioneering and challenging learning system for foreign language learning. Therefore, The proposed system should require experimenting and testing to validate its effectiveness with various different groups. At present, our service is in open beta [17] and validation

experiments are in progress with university students. ERP(Event Related Potential) experiments are being done to observe participant brain pattern variations during learning. Also there are several plans being considered for application of the proposed learning system.

Acknowledgements

Most of this paper was presented at the conference, APIC-ICONI2009 in Dec. 2009.

References

1. Jeon, H.C., Kim, K.W.: Economics of English. Samsung Economic Reasearch Institute (2006)
2. 2006 KOREA English report, The Korea Association of Teachers of English and MBC (2006)
3. Educational Testing Service, ETS, http://www.etc.org
4. Educational Testing Service, TOFLE, http://www.toefl.org
5. WordPress, South Koreas World Ranking on TOEFL Test, http://blog.educationusa.or.kr/2009/04/south-koreas-world-ranking-on-toefl-test/ (retrieved May 09, 2008)
6. Kim, K.H.S., Relkin, N.R., Lee, K.M., Hirsch, J.: Distinct cortical areas associated with native and second languages. Nature 388, 171–174 (1997)
7. Google, Google AJAX APIs, http://code.google.com/apis/ajax/ (retrieved May 09, 2001)
8. Wikipedia, Ajax(programming) (retrieved July 28, 2009)
9. Wikipedia, Computer-assisted language learning (retrieved July 28, 2009)
10. Cerego, Smart.fm, http://smart.fm/
11. Lexia Learning Systems, Lexia, http://www.lexialearning.com
12. Gi-zen, L.: Innovation research topics in learning technology: Where are the new blue oceans? British Journal of Educational Technology 39(4) (2008)
13. Mayes, J.T., Fowler, C.J.: Learning technology and usability: a framework for understanding courseware. Interacting with Computers 11(5), 485–497 (1999)
14. Durgunoglu, A.Y.: Cross-linguistic transfer in literacy development and implications for language learners. Annals of Dyslexia 52, 189–204 (2002)
15. Dickinson, D., McCabe, A., Clark-Chiarelli, N., Wolf, A.: Cross-linguistic transfer in literacy development and implications for language learners. Annals of Dyslexia 52, 189–204 (2002)
16. Nerbonne, J., Dokter, D., Smit, P.: Morphological processing and Computer-Assisted Language Learning. Computer Assisted Language Learning 11(5), 543–559 (1998)
17. English Brain Enhancement, English Brain Enhancement, http://ct.korea.ac.kr

Autonomic Resources Management of CORBA Based Systems for Transportation with an Agent

Woonsuk Suh[1] and Eunseok Lee[2]

[1] National Information Society Agency,
NIA Bldg, 77, Mugyo-dong Jung-ku Seoul, 100-775, Korea
sws@nia.or.kr
[2] School of Information and Communication Engineering, Sungkyunkwan University
300 Chunchun Jangahn Suwon, 440-746, Korea
eslee@ece.skku.ac.kr

Abstract. The application of advanced communications, electronics, and information technologies to improve the efficiency, safety, and reliability of transportation systems is commonly referred to as ITS. The core functions of the ITS are collection, management, and provision of real time transport information, and it can be deployed based on the Common Object Request Broker Architecture (CORBA) of the Object Management Group (OMG) efficiently because it consists of many interconnected heterogeneous systems. Fault Tolerant CORBA (FT-CORBA) supports real time requirement of transport information stably through redundancy by replication of server objects. However, object replication, management, and related protocols of FT-CORBA require extra system CPU and memory resources, and can degrade the system performance both locally and as a whole. This paper proposes an improved architecture to enhance performance of FT-CORBA based ITS by generating and managing object replicas adaptively during system operation with an agent. The proposed architecture is expected to be applicable to other FT-CORBA based systems.

Keywords: Agent, CORBA, Fault Tolerance, Performance.

1 Introduction

The key component of ITS is information systems to provide transport information in real time which have characteristics as follows. First, these systems run on nationwide communication networks because travelers pass through many regions to reach their destinations. Second, travelers should be able to receive real time information from many service providers, while driving at high speed and transport information should be able to be collected and transmitted to them in real time. Third, the update cycle of transport information to travelers is 5 minutes.

The ITS is deployed by various independent organizations and therefore is operated on heterogeneous platforms to satisfy the characteristics, functions, and performance requirements described earlier. FT-CORBA with stateful failover is needed to satisfy real time requirements of transport information considering the update cycle of 5 minutes. In stateful failover, checkpointed state information is periodically sent to

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 385–394, 2010.

the standby object so that when the object crashes, the checkpointed information can help the standby object to restart the process from there [16]. FT-CORBA protocols need additional CORBA objects such as the Replication Manager and Fault Detectors, server object replicas, and communications for fault tolerance, and therefore require accompanying CPU and memory uses, which can cause processing delays, thereby deteriorating the performance. Processing delay can be a failure for real time services of transportation information. This paper proposes an agent based architecture to enhance the performance of FT-CORBA based ITS. Due to the real time and composite characteristics of ITS, the proposed architecture is expected to be applicable to most applications. In section 2, CORBA based ITS and FT-CORBA related work are presented. In section 3, the proposed architecture introduces an agent to enhance performance of FT-CORBA based ITS. In section 4, the performance of the proposed architecture is evaluated by simulation focused on usage of CPU and memory. In section 5, this research is concluded and future research directions are presented.

2 Related Work

There are several representative CORBA based ITS worldwide. The Beijing Traffic Management Bureau (BTMB) in China had built an ITS using IONA's Orbix 2000 for the 2008 Olympic Games [9]. The Los Angeles County in US coordinates multiple traffic control systems (TCSs) on its arterial streets using a new Information Exchange Network (IEN) whose network backbone is CORBA software [3]. The Dublin City Council in Ireland has selected IONA Orbix™ as the integration technology for an intelligent traffic management system [9]. The Land Transport Authority in Singapore performed the 'traffic.smart' project, which is based on CORBA [8]. The Incheon International Airport Corporation in Korea had built information systems including ITS based on IONA Orbix 2.0 [10].

The Object Management Group (OMG) established the FT-CORBA which enhances fault tolerance by creating replicas of objects in information systems based on the CORBA. The standard for FT-CORBA aims to provide robust support for applications that require a high level of reliability, including applications that require more reliability than can be provided by a single backup server. The standard requires that there shall be no single point of failure. Fault tolerance depends on entity redundancy, fault detection, and recovery. The entity redundancy by which this specification provides fault tolerance is the replication of objects as mentioned earlier. This strategy allows greater flexibility in configuration management of the number of replicas, and of their assignment to different hosts, compared to server replication [15].

End-to-end temporal predictability of the application's behavior can be provided by existing real-time fault tolerant CORBA works such as MEAD and FLARe [1][2][12]. However, they also adopt replication styles of FT-CORBA mentioned earlier as they are. Active and passive replications are two approaches for building fault-tolerant distributed systems [5]. Prior research has shown that passive replication and its variants are more effective for distributed real time systems because of its low execution overhead [1]. In the WARM PASSIVE replication style, the replica group contains a single primary replica that responds to client messages. In addition, one or more backup replicas are pre-spawned to handle crash failures. If a primary fails, a

backup replica is selected to function as the new primary and a new backup is created to maintain the replica group size above a threshold. The state of the primary is periodically loaded into the backup replicas, so that only a (hopefully minor) update to that state will be needed for failover [7]. The WARM_PASSIVE replication style is considered appropriate in ITS in terms of service requirements and computing resource utilization. In practice, most production applications use the WARM PASSIVE replication scheme for fault tolerance. It is recommended in the field of logistics according to FT-CORBA specification as well. However, a method is required to maintain a constant replica group size efficiently.

FT-CORBA protocols need additional CORBA objects such as the Replication Manager and Fault Detectors, server object replicas, and communications for fault tolerance, and therefore require accompanying CPU and memory uses, which can cause processing delays, thereby deteriorating the performance. Processing delay can be a failure for real time services of transportation information. Natarajan et al. [14] have studied a solution to dynamically configure the appropriate replication style, monitoring style of object replicas, polling intervals and membership style. However, a method to maintain minimum number of replicas dynamically and autonomously, which means adjusting "a threshold" specified in the warm passive replication style for resource efficiency and overhead reduction of overall system, needs to be developed and improved.

3 Proposed Architecture

The FT-CORBA can be represented as Fig. 1 when an application uses the WARM PASSIVE style.

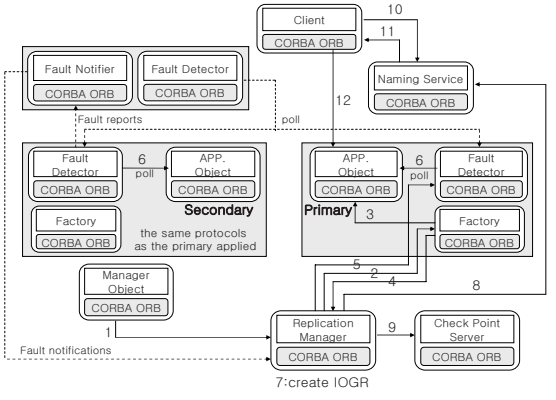


Fig. 1. FT-CORBA Protocol

The processes of Fig. 1 are summarized as follows [13]. 1. An application manager can request the Replication Manager to create a replica group using the create object operation of the FT-CORBA's Generic Factory interface and passing to it a set of fault tolerance properties for the replica group. 2. The Replication Manager, as

mandated by the FT-CORBA standard, delegates the task of creating individual replicas to local factory objects based on the Object Location property. 3. The local factories create objects. 4. The local factories return individual object references (IORs) of created objects to the Replication Manager. 5. The Replication Manager informs Fault Detectors to start monitoring the replicas. 6. Fault Detectors polls objects periodically. 7. The Replication Manager collects all the IORs of the individual replicas, creates an Interoperable Object Group References (IOGRs) for the group, and designates one of the replicas as a primary. 8. The Replication Manager registers the IOGR with the Naming Service, which publishes it to other CORBA applications and services. 9. The Replication Manager checkpoints the IOGR and other state. 10. A client interested in the service contacts the Naming Service. 11. The Naming Service responds with the IOGR. 12. Finally, the client makes a request and the client ORB ensures that the request is sent to the primary replica. The Fault Detector, Application Object, and Generic Factory in Fig. 1 are located on the same server.

The administrator of ITS can manage numbers of object replicas with the application manager in Fig. 1 by adjusting fault tolerance properties adaptively. However, administration of ITS needs to be performed autonomously and adaptively with minimal intervention by the administrator. In addition, the use of system CPU and memory resources in FT-CORBA is large, which can affect the real time characteristics of ITS due to processing delays because FT-CORBA is an architecture to enhance fault tolerance based on the redundancy of objects. Accordingly, it is possible to enhance efficiency and prevent potential service delays if an autonomous agent (FTAgent) is introduced to the FT-CORBA based ITS, which adjusts the minimum numbers of object replicas autonomously and adaptively. It can be applied to other applications based on FT-CORBA. An autonomous agent is a system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda, and so as to effect what it senses in the future [6]. The FTAgent has algorithm and database [11] which can help to maintain the number of replicas efficiently because they require system CPU and memory resources both directly and indirectly, which can lower performance in terms of the overall ITS as mentioned earlier. The FTAgent is introduced in Fig. 2 on the same system as the Replication Manager in Fig. 1 which maintains 3 replicas for each object in this paper, i.e., the primary, first secondary, and second secondary replicas.

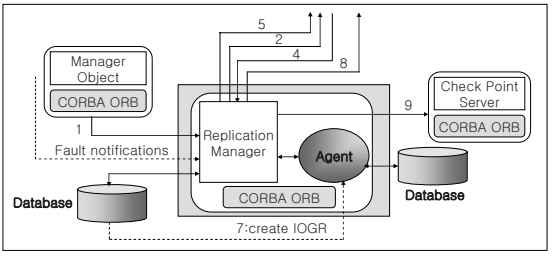


Fig. 2. Architecture to improve FT-CORBA

The FTAgent maintains its DB to support the Replication Manager for management of object replicas whose schema is as shown in Table 1.

Table 1. DB maintained by the FTAgent

IOGR IDs	date(dd/mm/yy)	time	failure 1	failure 2	flag	$risky_k$	NoROR
1	01/01/08	00:00:00~00:04:59	0	0	0	0	0
.	.	.	.	.	.	.	.
100	31/01/08	23:55:00~23:59:59	0	1	0	0	1

The IOGR IDs identify replica groups of each object whose numbers are 100 in this paper. The numbers of records in Table 1 are maintained to be under 1 million because values of the time attribute of Table 1 are measured by 5 minutes per day. The date identifies days of one month. The time is measured every 5 minutes. The failure 1 means failures of primary object replicas which are original or recovered from previous failures. The failure 2 means failures of first secondary replicas after becoming the primary ones. The values of failure 1 and 2 are 0 for working and 1 for failed, respectively. The flag has two values which are 0 when primary or first secondary is working and 1 when both primary and first secondary have failed for respective 5 minutes as a service interval. The $risky_k$ is a fault possibility index for object groups, which is assigned to each interval of 5 minutes for one hour backward from current time, and is set to zero at first. The k and $risky_k$ are equivalent and they ranges from 0 to 11 because the flag is set to 1 up to a maximum of 11 times for one hour. The values are assigned in the way that 11 and 0 are assigned to the nearest and furthest intervals of 5 minutes to current time, respectively.

The FTAgent searches the DB managed by Replication Manager and updates states (failed or working) of primary and first secondary replicas of each object (1~100) on its own DB in real time resuming every 5 minutes which ranges from previous to next middles of the information service interval of 5 minutes, restricted to one month (last 30 days) from current time. Search intervals are set between the respective middles of the former and latter service intervals because the moment of updating transport information is more important than any other time.

The FTAgent identifies whether there are simultaneous failures of primary and first secondary replicas of each object by searching its DB in real time. Object faults of ITS result from recent short causes rather than old long ones because it is influenced by road situations, weather, and traffic, etc., which vary in real time. If simultaneous failures for 5 minutes have originated for one month until now that the first secondary replica crashes, which has been promoted to the primary as soon as the original primary one has failed, and it is in the rush hours, the FTAgent requires the Replication Manager to adjust the number of replicas of relative objects to 3 or 2, otherwise to reduce it to 2. In other words, the FTAgent lets the Replications Manager adjust the number of object replicas autonomously and adaptively. The decision by the value of the parameter rush hours of whether it is in the rush hours is beyond this paper and depends on judgment in terms of traffic engineering. The algorithm of the FTAgent is described as follows.

```
FTAgent(int rush hours){
  while(there is no termination condition){
(1) search whether primary replicas of each object are
    working on the DB maintained by Replication Manager
    (RM) in real time resuming every 5 minutes which
    ranges from previous to next middles of the informa-
    tion service interval of 5 minutes, restricted to
    last 30 days from current time;
(2) if(primary replica is working){failure 1=0 for all
      object groups identified by IOGRs; flag=0;}
(3) else{failure 1=1 for all object groups;
(4)      confirm whether first secondary of each object pro-
         moted to primary by RM is working on the RM DB;
(5)      if(first secondary is working){failure 2=0;flag=0;}
(6)      else{failure 2=1;
(7)           confirm whether the replica created by RM,
              substituting for crashed primary is working;
(8)           if(it is working){failure 1=0; flag=0;}
(9)           else flag = 1;}}
(10)Decision_Number_of_Replicas(rush hours);}}

Decision_Number_of_Replicas(int rush hours){
(11)an array for numbers of two successive 1's of flag
    values for all object groups=0;
(12)search successions of two 1's in flag values for all
    object groups;
(13)if(there are two successive 1's of flag values) add
    to the number of two successive 1's of flag values
    for relevant objects;
(14)if{(number of two successive 1's ≥ 1 for last one
       hour)and(rush hours)}{
(15)  NoROR=[3-3 x {max(risky_k)/11}]/3;NoROR_1=NoROR;
(16)  if(0≤k≤5){NoROR = {Σ_{d=1}^{30}(d × NoROR_d)}/30/30; NoROR_2 = NoROR;}
(17)  select the smaller one between NoROR_1 and NoROR_2,
      round it off, and assign the result to NoROR;
(18)  let RM keep the number of relevant object replicas
      minus NoROR, whose selection is the order of their
      ID numbers;}
(19)else if{(number of separate 1's≥2 for last one
      hour)and(rush hours)}{
(20)  if(min|t_i-t_j|<5minutes)let RM keep the number of
        relevant object replicas 3;
(21)  else let RM reduce the number to 2;}
(22)else let RM reduce the number to 2 which mean the two
    of the 3 replicas which are working at the moment
    and whose priority for selection is the order of
    their ID numbers;}
```

In line (15), NoROR stands for the number of reduced object replicas and in line (16), $NoROR_d$ means the minimum number of reduced object replicas in the time slots of 5 minutes at each day for last 30 days. In line (20), t_i and t_j mean the time when flag values are 1, respectively. The proposed architecture in this paper can be applied to the work such as MEAD and FLARe to increase resource availability and decrease overheads by enhancing utilization efficiency of CPU and memory, thereby improving end-to-end temporal predictability of the overall system.

4 Evaluations

The items for performance evaluation are total time of CPU use and maximum usage of memory of servers related to the 11 processes except for the 12^{th} process in Fig. 1 from the beginning to termination of the simulation of two types to maintain 3 and 2 object replicas for fault tolerance [4]. The simulation has been performed on the PC with Intel Pentium M Processor 1.60 GHz, 1.0 GB memory, and Windows XP as the OS. The programs are implemented in Visual C++ 6.0. Firstly, the use rate of CPU during simulation is 100% on the implementation environment, and therefore it is appropriate to measure and compare total times of CPU use from beginning to termination of the simulation programs of two types. They must be measured for all servers related to creation and maintenance of object replicas in Fig. 1. The processes without numbers on arrows in Fig. 1 are not considered. Accordingly, the number of CPUs to be considered is 11.

Secondly, the peak usage is more appropriate for memory rather than continuous measurement of memory use. Therefore, the maximum usage of two types of 3 and 2 replicas is measured respectively. Total time of CPU use and maximum usage of memory are compared in that the Replication Manager maintains 3 and 2 replicas of objects respectively. Namely, the 11 processes prior to the client requesting services in Fig. 1 are simulated with 2 separate programs which describe the two types in terms of CPU and memory use. The components of the FT-CORBA are the same and therefore they are not designed in the programs in terms of memory use. The processing latencies with loops in the programs are set for the type of 3 replicas as follows: 1) latency between internal components: 2 sec. 2) latency between external components: 3 sec. 3) latency for the FTAgent to search the DB maintained by the Replication Manager and itself and to deliver related information to it : 5 sec. Of course, latencies directly related to creating and maintaining 2 replicas are set to two thirds of those for 3 replicas. The values of the established processing latencies are variable due to basic processes of the OS in the implementation environment, which is ignored because the variableness originates uniformly in simulations of both types to be compared. The conditions presented earlier are based on the experimental fact that the processing latency to select records which have the condition of the line (14) in the algorithm is about 3 seconds in case of the Oracle 9i DBMS which maintains 1 million records with 13 columns on IBM P650 with 4 CPUs of 1.24GHz and 12GB memory, and is 34 Km distant from a client.

A commercial internet browser is used as an object to simulate usage of CPU and memory in creation and termination of 3 and 2 object replicas obviously. The browser is called 3 and 2 times by types and kept as processes until the simulation is finished.

The items to be compared are total time of CPU use and maximum usage of memory from the beginning to termination of the simulation as mentioned earlier. The types of 3 and 2 replicas are simulated respectively by executing the relevant programs 5 times where http://www.ieee.org is filled in the URL of the browser assumed as an object. The results for the total CPU time used are shown in Fig. 3.

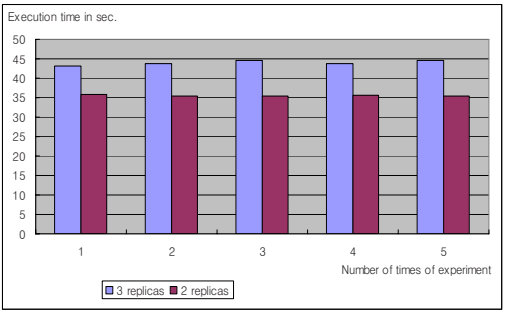


Fig. 3. Total time of CPU use in sec.

The total time of CPU use ranges from 43.36 to 44.02 seconds for the type of 3 replicas. The arithmetic mean is 43.55 seconds and the standard deviation is 0.27 seconds, which is 0.6% based on the minimum of 43.36 seconds. On the other hand, the total time of CPU use ranges from 35.42 to 36.67 seconds for the type of 2 replicas. The arithmetic mean is 35.77 seconds and the standard deviation is 0.51 seconds, which is 1.4% based on the minimum of 35.42 seconds. The deviations result from basic processes of Windows XP, the properties of processed data, and a variable network situation, which causes deviations because the browser is used as an object. The performance improvement in terms of CPU is 17.86% through comparison of the values of the two arithmetic means. Accordingly, the improvement ranges from 0 to 17.86% whose lower and upper bounds correspond to simultaneous failures of 100% and 0% of primary and first secondary replicas, respectively. Therefore, the expected improvement is the arithmetic mean of 8.93% assuming the ratio of simultaneous failures of primary and first secondary replicas is 50% over all objects.

The results for maximum usage of memory are shown in Fig. 4.

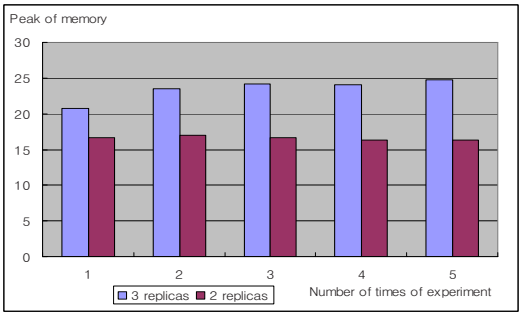


Fig. 4. Maximum usage of memory in MB

The peak of memory usage ranges from 27.09 to 28.85 MB for the type of 3 replicas. The arithmetic mean is 27.83 MB and the standard deviation is 0.65 MB, which is 2.4% based on the minimum of 27.09 MB. On the other hand, the peak of memory usage ranges from 22.64 to 24.87 MB for the type of 2 replicas. The arithmetic mean is 23.66 MB and the standard deviation is 0.79 MB, which is 3.5% based on the minimum of 22.64 MB. The deviations result from the same causes as in case of CPU described earlier. The performance improvement in terms of memory is 14.98% through comparison of the values of the two arithmetic means. Accordingly, the improvement ranges from 0 to 14.98% whose lower and upper bounds correspond to simultaneous failures of 100% and 0% of primary and first secondary replicas respectively. Therefore, the expected improvement is the arithmetic mean of 7.49% assuming the ratio of simultaneous failures of primary and first secondary replicas is 50% over all objects.

The simulation has been performed with another URL of www.springer.com to investigate how much the properties of processed data and a variable network situation influence the results. The total CPU time used ranges from 43.59 to 44.44 seconds for the type of 3 replicas. The arithmetic mean is 44.06 seconds. On the other hand, the total time of CPU use ranges from 35.64 to 36.55 seconds for the type of 2 replicas. The arithmetic mean is 35.9 seconds. The performance improvement in terms of CPU is 18.52% through comparison of the values of the two arithmetic means. Accordingly, the improvement ranges from 0 to 18.52%. Therefore, the expected improvement is 9.26% which is 0.33% higher than that with the previous URL. The peak of memory usage ranges from 41.98 to 50.82 MB for the type of 3 replicas. The arithmetic mean is 46.22 MB. On the other hand, the peak of memory usage ranges from 33.76 to 36.32 MB for the type of 2 replicas. The arithmetic mean is 35.56 MB. The performance improvement in terms of memory is 23.06% through comparison of the values of the two arithmetic means. Accordingly, the improvement ranges from 0 to 23.06%. Therefore, the expected improvement is 11.53% which is 4.04% higher than that with the previous URL. To sum up, the influence of the properties of processed data and a variable network situation on the ratio of performance improvement in terms of CPU and memory is not abnormal although there is a difference in memory.

5 Conclusion

The ITS can be deployed based on FT-CORBA efficiently considering heterogeneous and real time properties of it. However, improvement is needed to enhance performance of the ITS based on FT-CORBA because it requires additional uses of CPU and memory for object redundancy. This paper has proposed an architecture to adjust the number of object replicas autonomously and adaptively with an agent of the FTAgent. In the future, additional research is needed to optimize the number of object replicas in real environment of ITS as follows. Firstly, the FTAgent can improve performance of its own over time by learning from statistical data related to recovery of replicas by objects such as the interval to check failures and their frequency, which means improvement of the line (14) through (22) of the algorithm. Secondly, the size of the DB maintained by the FTAgent has to be studied experimentally as well which is the record of failures for one month in this paper. It will be decided according to the characteristics of transportation information which generates in real time. The proposed

architecture can be applied to other FT-CORBA based systems because the ITS is a composite one to have properties of most applications.

References

1. Balasubramanian, J., Gokhale, A., Schmidt, D.C., Wang, N.: Towards Middleware for Fault-tolerance in Distributed Real-time and Embedded Systems. In: Meier, R., Terzis, S. (eds.) DAIS 2008. LNCS, vol. 5053, pp. 72–85. Springer, Heidelberg (2008)
2. Balasubramanian, J., Tambe, S., Lu, C., Gokhale, A.: Adaptive Failover for Real-time Middleware with Passive Replication. In: 15th Real-time and Embedded Application Symposium, pp. 1–10. IEEE, Los Alamitos (2009)
3. County of Los Angeles Department of Public Works, `http://www.ladpw.org/TNL/ITS/IENWeb/index.cfm`
4. FatihAkay, M., Katsinis, C.: Performance improvement of parallel programs on a broadcast-based distributed shared memory multiprocessor by simulation. Simulation Modelling Practice and Theory 16(3), 347–349 (2008)
5. Felber, P., Narasimhan, P.: Experiences, Approaches and Challenges in building Fault-tolerant CORBA Systems. Transactions of Computers 54(5), 497–511 (2004)
6. Franklin, S., Graesser, A.: Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. In: Jennings, N.R., Wooldridge, M.J., Müller, J.P. (eds.) ECAI-WS 1996 and ATAL 1996. LNCS, vol. 1193, p. 25. Springer, Heidelberg (1997)
7. Gokhale, A., Natarajan, B., Schmidt, D.C., Cross, J.: Towards Real-time Fault-Tolerant CORBA Middleware. Cluster Computing: the Journal on Networks, Software, and Applications Special Issue on Dependable Distributed Systems 7(4), 15 (2004)
8. Guan, C.C., Li, S.L.: Architecture of traffic.smart. In: 8th World Congress on ITS, pp. 2–5. ITS America, Washington (2001)
9. IONA Technologies, `http://www.iona.com/`
10. Lee, J.K.: IICS: Integrated Information & Communication Systems. Journal of Civil Aviation Promotion 23, 71–80 (2000)
11. Nagi, K., Lockemann, P.: Implementation Model for Agents with Layered Architecture in a Transactional Database Environment. In: 1st Int. Bi-Conference Workshop on Agent Oriented Information Systems (AOIS), pp. 2–3 (1999)
12. Narasimhan, P., Dumitras, T.A., Paulos, A.M., Pertet, S.M., Reverte, C.F., Slember, J.G., Srivastava, D.: MEAD: support for Real-Time Fault-Tolerant CORBA. Concurrency And Computation: Practice And Experience 17(12), 1533–1544 (2005)
13. Natarajan, B., Gokhale, A., Yajnik, S.: DOORS: Towards High-performance Fault Tolerant CORBA. In: 2nd Distributed Applications and Objects (DOA) conference, pp. 1–2. IEEE, Los Alamitos (2000)
14. Natarajan, B., Gokhale, A., Yajnik, S., Schmidt, D.C.: Applying Patterns to Improve the Performance of Fault Tolerant CORBA. In: 7th International Conference on High Performance Computing, pp. 11–12. ACM/IEEE (2000)
15. Object Management Group.: Fault Tolerant CORBA. CORBA Version 3.0.3 (2004)
16. Saha, I., Mukhopadhyay, D., Banerjee, S.: Designing Reliable Architecture For Stateful Fault Tolerance. In: 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2006), p. 545. IEEE Computer Society, Washington (2006)

Performance Evaluation of a Reservoir Simulator on a Multi-core Cluster

Carolina Ribeiro Xavier[1], Elisa Portes dos Santos Amorim[1],
Ronan M. Amorim[1], Marcelo Lobosco[1],
Paulo Goldfeld[2], Flavio Dickstein[2],
and Rodrigo Weber dos Santos[1]

[1] Dept. of Computer Science, Federal University of Juiz de Fora
Juiz de Fora, MG, Brazil
[2] Dept. of Applied Mathematics, Federal University of Rio de Janeiro
Rio de Janeiro, RJ, Brazil
{carolrx,elisaufjf,ronanrmo}@gmail.com, {flavio,goldfeld}@labma.ufrj.br,
{rodrigo.weber,marcelo.lobosco}@ufjf.edu.br

Abstract. Reservoir simulators are one of the most important tools on reservoir engineering since they allow the prediction of real reservoir's behavior. However, in order to deal with medium and large scale problems it is necessary to use parallel computing. This work presents the development of a reservoir simulator, based on a two-phase flow model of porous media, and its parallelization. The implementation of the simulator was based on an IMPES scheme and the PETSc library, which uses MPI for data communication between processes, was employed to solve the system of equations. The performance analysis was made in a parallel environment composed by a cluster of multiprocessor computers and the results suggest that the performance of parallel applications strongly depends on the memory contention in multiprocessor computers, such as the quad-cores. Thus, parallel computing should follow certain restrictions regarding the use and mapping of tasks to compute cores.

Keywords: Reservoir simulation, MPI, multi-core.

1 Introduction

Reservoir engineering is a branch of petroleum engineering that applies scientific principles to the flow problems arising during the production of oil and gas so as to obtain a high economic recovery.

Reservoir simulation is a powerful tool that has been extensively used in reservoir engineering. It combines physics, mathematics, reservoir engineering and computer programming. One of the main goals of the models is to have the the ability to predict the behavior of a reservoir.

The model that represents such phenomena is quite complex, involving the solution of a nonlinear system of partial differential equations which leads to an

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 395–408, 2010.

expensive computational effort. A parallel version of the simulator was implemented in order to reduce the execution time. The evaluation of this parallel implementation was performed in a cluster of multiprocessor computers.

In the last decade, many studies have analyzed parallel algorithms and high performance platforms based on computer clusters. Currently, new high performance technologies and architectures are emerging, such as FPGAs [11], computational grids [15], GPUs and multi-core processors, which may be homogeneous or heterogeneous (such as Cell processor).

For each of these technologies there are examples of success in the literature, presenting applications that had their execution times substantially reduced. In this work, we evaluate how the parallel reservoir simulator behaves in a cluster of multiprocessor computers.

This work is organized as follows: Section 2 introduces the problem formulation. Section 3 introduces multi-processors theory. Section 4 presents the serial and parallel implementation. Section 5 presents the methods and the computer platform used for the tests. Sections 6, 7 and 8 present the results discussion and conclusion of this work, respectively.

2 The Problem

2.1 Theory

The problem treated in this paper is a two dimensional two-phase (water/oil) incompressible and immiscible porous media flow in a gravity-free environment [6]. The system of partial differential equations which governs this flow is derived from the *law of mass conservation* and the *Darcy Law*. The law of mass conservation for both phases is written as $\phi\partial_t(\rho_\alpha s_\alpha) + \nabla.(\rho_\alpha v_\alpha) = Q_\alpha$, where $\alpha = w$ denotes the water phase, $\alpha = o$ denotes the oil phase, ϕ is the porosity of the porous medium, and ρ_α, s_α, v_α and Q_α are, respectively, the density, saturation, volumetric velocity and flow rate in wells of the α-phase. The volumetric velocity (v_α) is given by the Darcy law: $v_\alpha = \frac{Kk_{r\alpha}(s_\alpha)}{\mu_\alpha}\nabla p_\alpha$, where K is the effective permeability of the porous medium, $k_{r\alpha}$ is the relative permeability of α-phase, which is a function that depends on saturation, and μ_α and p_α are, respectively, viscosity and pressure of the α-phase. In this work we consider that the capillary pressure is null, that is, $p_w = p_o$. So, from now on we will refer to pressure simply as p. We also have that $s_w + s_o = 1$. We introduce the phase mobility and transmissibility functions, respectively: $\lambda_\alpha(s) = \frac{k_{r\alpha}(s)}{\mu_\alpha}$, $T_\alpha(s) = K\lambda_\alpha$, where $s = s_w$ from now on. The volumetric velocity can then be written as $v_\alpha = -T_\alpha\nabla p$. We assume that the phases density and viscosity are constant and get

$$\begin{cases} \phi\rho_w\partial_t s_w + \rho_w\nabla v_w = Q_w \\ \phi\rho_o\partial_t s_o + \rho_o\nabla v_w = Q_o\ . \end{cases} \tag{1}$$

Now we can divide the equations in 1 by ρ_α and sum both and get

$$\begin{cases} \phi\partial_t s + \nabla v_w = q_w \\ \nabla v_t = q_t\ . \end{cases} \tag{2}$$

where $q_\alpha = \frac{Q_\alpha}{\rho_\alpha}$ is the flow rate density of α-phase, $q_t = q_w + q_o$ and $v_t = v_w + v_o$. Defining total mobility as $\lambda_t = \lambda_w + \lambda_o$ we introduce the fractional flow functions as $f(s) = \frac{T_w}{T_t} = \frac{\lambda_w}{\lambda_t}$. System 1 is then rewritten as

$$\begin{cases} \phi \partial_t s - \nabla(f(s) T_t(s) \nabla p) = q_w \\ -\nabla(T_t(s) \nabla p) = q_t \ . \end{cases} \tag{3}$$

To complete the model the boundary conditions must be specified. In this paper we consider no flow boundary condition, $v_\alpha . \nu = 0, x \in \partial\Omega$, where ν is the outer unit normal to the boundary $\partial\Omega$ of the domain Ω. Finally we define the initial condition given by $s(x, 0) = s_0(x), x \in \Omega$.

The forward problem treated on this paper is the system of partial differential equations given by 3 with the boundary and initial conditions given above.

3 Clusters of Multiprocessor Computers

The main goal when using parallel computing is to reduce the processing time of the task. However, the way such a mechanism is implemented may vary and it is directly related to the hardware available since hardware characteristics have implications on algorithm design.

The cluster is perhaps one of the most popular parallel architectures. A cluster of computers is a group of connected computers that in many aspects seems to be a single computer. One can build a cluster of uniprocessors, multiprocessors or a mix of them. Since the multi-core machines are widespread, multiprocessor (or multi-core) clusters are the current standard. Figure 1 presents a simplified representation of a cluster of multiprocessor computers.

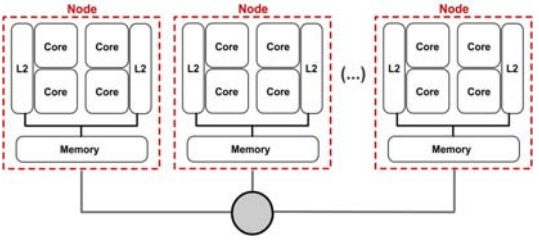


Fig. 1. Simplified representation of a cluster of multiprocessor computers

The way processes communicate constitutes an important issue in the implementation of an effective environment for high-performance computing. Three basic approaches can be used for inter-process communication, namely shared memory, message passing, or a combination of both. Parallel programs have evolved using message passing libraries, such as the Parallel Virtual Machine (PVM) [4] and the Message Passing Interface (MPI) [5], as their main method of communication. In this case, the programmer is responsible for data communication and synchronization among the nodes running an application. In shared

memory systems, processes share data easily by changing the contents of shared memory locations. Both approaches can be implemented on systems with various architectures: on clusters, on SMPs, or even on single CPU machine. For example, in distributed shared memory (DSM) systems, processes share data transparently across node boundaries; data faulting, location, and movement is handled by the underlying system. Treadmarks [27] and HLRC [26] are examples of state-of-the-art software DSM systems. In the same way, message passing can be used to communicate distinct processes in the same computer.

At first, it seems that communication is far more efficient in shared memory systems, since the network latency is eliminated. However, it can be also quite troublesome. To begin with, synchronization is necessary to avoid race conditions. Also, two or more cores/processors can simultaneously try to access the memory, which will impose a serialization on memory access. Both situations can severally hurt performance since in the worst case the core/processor must stall while waiting for a) synchronization or b) the completion of a memory access made by another core/processor. It should be stressed that this situation can also occur in applications that use memory passing paradigm on top of a multiprocessor computer. If a process needs to send a message to another process, this message will be written in an output buffer located at the memory. Then, the message will be copied to the input buffer of the destination process, that will read the memory to access the message. Thus, a memory contention can occur if two or more processes try to send or receive a message at the same time.

On clusters of multiprocessor computers, a message can be exchanged in different ways. If the processes are located in distinct nodes, the message is copied to an output buffer of the origin process, then it travels through the network and it is copied to an input buffer of the destination process. If the processes are located in the same node, the message does not travel through the network, but is passed from one process to another using the memory.

4 Implementation

The differential equations described in Sect. 2.1 are nonlinear and coupled. In this work the method used to solve these equations is the so called IMPES. Our implementation of the IMPES methods adopts an adaptive time step scheme. The basic idea of the IMPES method is to separate the computation of pressure from that of saturation. The coupled system is split into a pressure equation and a saturation equation, and the pressure and saturation equations are solved using implicit and explicit time approximation approaches, respectively. Decoupling the system (3) we get an elliptic equation for pressure given by (4) and a nonlinear hyperbolic equation for saturation, given by (5).

$$-\nabla(T_t(s)\nabla p) = q_t \ . \tag{4}$$

$$\phi\partial_t s - \nabla(f(s)T_t(s)\nabla p) = q_w \ . \tag{5}$$

For the pressure computation, the saturation s in (4) is supposed to be known and (4) is solved implicitly for p. In this work, the finite volume method was used for spatial discretization [1]. As mentioned before, the saturation equation given by (5) is solved explicitly. The IMPES method goes as follows: given s^0; for $n = 0, 1, ...$ we use (4) and s^n to evaluate p^n; next we use (5), s^n and p^n to evaluate s^{n+1}. To guaranty the stability of this equation the time step Δt must be sufficiently small which is an expensive requirement. To minimize this problem, we actually used an Improved IMPES method [2]. This method uses the fact that pressure changes less rapidly in time than saturation. Knowing this, it is appropriate to take a much larger time step for the pressure than for the saturation. Using the Improved IMPES method we have two different time steps: Δt^n for pressure and $\Delta t^{n,l}$ for saturation. Pressure p^n corresponds to instant $t^n = \sum_{1<=i<=n} \Delta t^i$ and saturation $s^{n,l}$ corresponds to instant $t^{n,l} = t^n + \sum_{1<=j<=l} \Delta t^{n,j}$. We deduced the CFL conditions given by the next two equations. One for cells that have injector wells $\Delta t^{n,l} \leq \frac{\phi(1-s_{o,res}-s_{i,j}^{n,l})}{\beta_1 q_w^{n,l}(1-f(s_{i,j}^{n,l}))}$, where $\beta_1 > 1$ and another to the other cells, given by $max f'(s_m) \sum_m \frac{\Delta t^{n,l}}{\phi \Delta_m} |v_m^n| \leq \beta_2$, where $0 < \beta_2 < 1$ and m corresponds to interfaces where the flow enters the block. To control the pressure time step Δt^n we calculate the pressure variation percentage $VP^n = \frac{||p^{n+1}-p^n||}{||p^n||}$. If VP^n is greater than a given VP_{max} pressure time is reduced and if it is less then a given VP_{min}, it is increased.

4.1 Parallel Implementation

The parallelization of the simulator was done in two steps. The first step was to parallelize the solution of the pressure equation, and second one to parallelize the solution of the saturation equation.

The parallelization of the solution of the pressure equation was perfomed using the PETSc libarry. The PETSc (*Portable, Extensible Toolkit for Scientific Computation*) library was used to solve the linear systems associated to the discretization of the Partial Differential Equations. PETSc is a suite of data structures and routines for the scalable (parallel) solution of scientific applications modeled by Partial Differential Equations. It employs the MPI standard for parallelism [3]. To solve the linear system associated to the discretzation of the pressure equation the Conjugate Gradient algorithm was used preconditioned by a ALgebraic Multigrid Method (AMG).

For the solution of the saturation equation, rows are distributed evenly to the processors. Each processor updates the saturation of their rows. Since we use a four neighbor stencil, after each update it is necessary to change the neighbors, called ghost points. For this reason each processor receives, in addition to their own rows, two additional ones: a) the last line of its upper neighbor and b) the first line of its lower neighbor. This situation is presented in Figure 2.

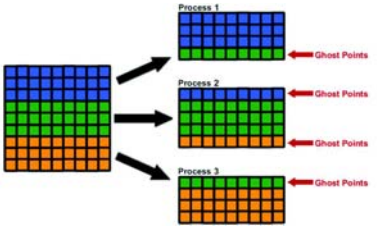


Fig. 2. The exchange of the values of ghost points

This parallelization scheme is called domain decomposition. The left side of Figure 2 shows the grid discretization of the reservoir and the right side shows how the distribution of the grid is made among the processes.

It is clear that in order for this algorithm to work, the rows must be updated at each time step, since at each time step the saturation values change. For this reason, it is necessary to proceed the exchange of rows among the neighbors at each time step. MPI was used to implement the data exchange.

We used C++ to implement the numerical solutions of both steps, and use Open MPI as their MPI communication layer. The Open MPI Project is an open source MPI-2 implementation that is developed and maintained by a consortium of academic, research, and industry partners.

5 Experimental Evaluation

The performance metric most commonly used to evaluate parallel applications is speedup, defined in [20] as $S(n,p) = \frac{T(n,1)}{T(n,p)}$, where n is the problem dimension and p o number of processes.

The ideal speedup is $S(n,p) = p$, but it is not always possible to achieve this value. This situation is related to an ever-increasing portion of time spent in communication and synchronization. Eventually, the overhead from communication and synchronization dominates the time spent solving the problem, which increases rather than decreases the amount of time required to finish. This situation is called slowdown.

In this work, the speedup was used to analyze the performance of our application in distinct scenarios.

The experimental results were obtained with an 4-node Linux cluster of 2.33 GHz Core2Quad®PCs, each of which with 4 GB RAM, 2 MB L2 cache and 160 GB disk. Each node was connected to a Gigabit Ethernet switch.

5.1 Methodology

The performance figures of the parallel simulator were collected by running a 5-spot pattern reservoir simulation model, which simulates 50 days of operation of an oil reservoir. Three different grid dimensions were used in our simulations: 101x101, 401x401 and 1001x1001.

In order to verify the scalability of the algorithm, we ran experiments comprising of 1 to 16 nodes on our cluster. The experiments were run with different mapping of the application tasks onto cores. We submitted the benchmark five times to our simulator, and reported the average execution time for each configuration. The standard deviation was very insignificant. The configurations are the following:

- 1_1: 1 process running on 1 machine
- 2_1: 2 processes running on 1 machine
- 2_2: 2 processes running on 2 machines
- 4_1: 4 processes running on 1 machine
- 4_2: 4 processes running on 2 machines
- 4_4: 4 processes running on 4 machines
- 8_2: 8 processes running on 2 machines
- 8_4: 8 processes running on 4 machines
- 16_4: 16 processes running on 4 machines

Figures 3, 4 and 5 illustrate the different configurations for executions with four processes. The cores highlighted in the figures represent the cores that have been allocated.

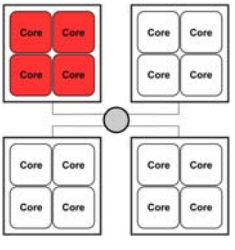


Fig. 3. 4_1 - 4 processes on 1 machine

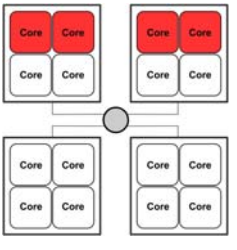


Fig. 4. 4_2 - 4 processes on 2 machines

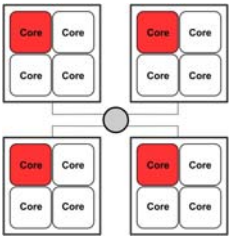


Fig. 5. 4_4 - 4 processes on 4 machines

6 Results

This section presents the results of simulations. Table 1 presents the execution times on the 101x101 grid and Figure 6 the speedup obtained.

As shown in Table 1 and Figure 6, our implementation is not efficient for the 101x101 grid. We can observe that the speedup was obtained only for two configurations: a) 2_1, i.e., two processes on one machine; and b) 4_1, suggesting that the low performance obtained is due to a remote communication overhead. It is important to note that the time spent to calculate the pressure was greater than to calculate the saturation, and the saturation speedup was much better than the pressure speedup, which directly affects the total simulator speedup.

Table 1. Execution times on the 101x101 grid (in seconds)

cores_ machines	1_1	2_1	2_2	4_1	4_2	4_4	8_2	8_4	16_4
Saturation	0,05	0,02	0,03	0,01	0,02	0,02	0,01	0,02	0,02
Pressure	0,76	0,5	2,71	0,32	1,74	1,03	1,75	1,87	1,85
Total	0,85	0,55	2,77	0,35	1,78	1,07	1,78	1,91	1,89

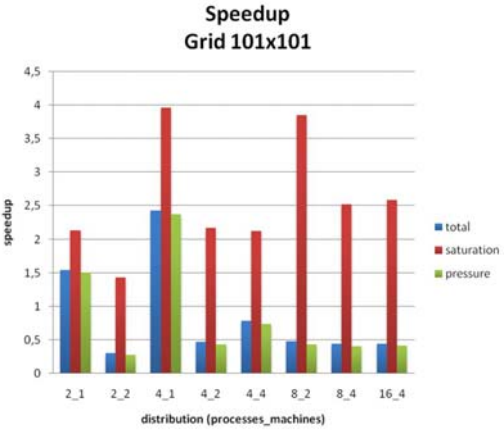


Fig. 6. Speedup on the 101x101 grid

As can be seen in Table 2 and Figure 7, our implementation performed better for the 401x401 grid than the previously one. If four processes are used, the better configuration is one in which the processes are distributed across four machines, followed by the one in which processes are distributed across two machines. The worst case is the configuration in which all processes are located in the same machine. A possible cause for this is due to memory contention.

Table 3 presents the execution times on the 1001x1001 grid and Figure 8 the speedup obtained. The speedups obtained were similar to the speedups obtained for the 401x401 grid.

This time, if four processes are used, the best configuration is the one in which the processes are distributed across two machines. Probably, this change occurred because the remote communication overhead overwhelmed the memory

Table 2. Execution times on the 401x401 grid (in seconds)

cores_ machines	1_1	2_1	2_2	4_1	4_2	4_4	8_2	8_4	16_4
Saturation	4,99	2,5	2,26	1,67	1,31	1,32	0,89	0,7	0,48
Pressure	101,19	69,58	68,85	67,93	43,6	41,77	36,65	24,35	22,39
Total	109,17	73,73	72,62	70,48	45,73	43,9	38,01	25,48	23,12

contention overhead. Again, the worst case is the configuration in which all processes are located in the same machine. It is also interesting to note that a superlinear speedup was achieved in some configurations.

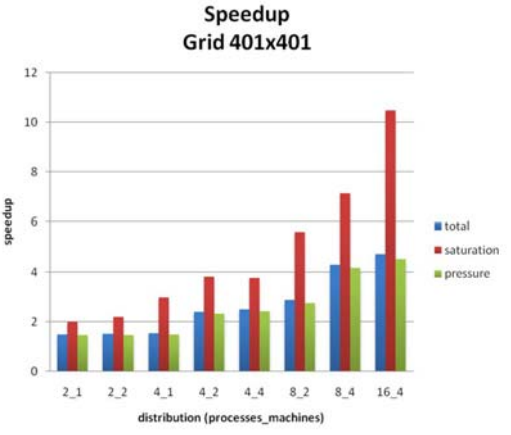


Fig. 7. Speedup on the 401x401 grid

Table 3. Execution times on the 1001x1001 grid (in seconds)

cores_ machines	1_1	2_1	2_2	4_1	4_2	4_4	8_2	8_4	16_4
Saturation	50,56	25,67	22,89	15,89	11,88	11,96	8,04	6,11	4,22
Pressure	926,09	699,04	555,22	766,12	412,7	425,94	393,47	218,38	199,59
Total	1002,24	738,4	590,98	791,23	432,51	445,85	406,25	228,53	206,17

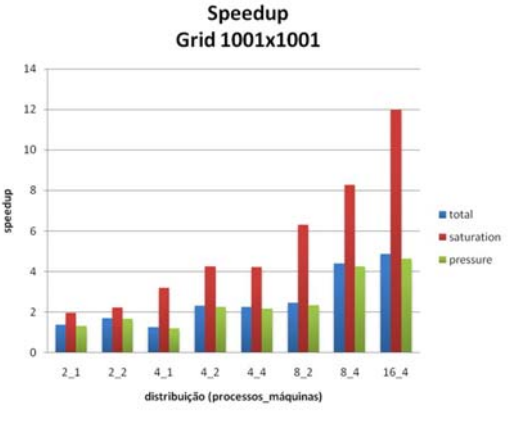


Fig. 8. Speedup on the 1001x1001 grid

7 Discussion

7.1 Parallel Simulator

To validate the parallel model, the saturation and the pressure values computed by the parallel simulator were compared to the values computed by the sequential version of the simulator that was previously validated. The obtained results, as expected, were identical.

With respect to the scalability of the model, first we should say that our cluster size limits our analysis. However, we observed that the solution of the saturation equation achieved good results, including the superlinear ones. However, the results were not that impressive for the solution of the pressure equation. The good results obtained in the saturation solution could be explained by the straightforward parallelization of the explicit equation and the limited ammount of communication (basically the exchange of ghost-points between neighboring nodes); whereas the solution of the system of linear equations demanded further communications, such as reduction (all-reduce) operations to implement the inner products of the Conjugate Gradient. In addition, the multigrid preconditioner operates on smaller linear systems, i.e. smaller grids. The parallel performance of the solution of these small systems is poor.

For small grids, such as 101x101 grid blocks, the parallel execution did not result in a significant reduction in computation time. However, in some cases, a speedup was obtained. This was the case of the following configurations: a) two process in the same machine and b) four process in the same machine. Probably, speedup was not obtained in other configurations due to the high communication overhead.

However this picture has changed considerably when a medium size grid was evaluated. For the 401x401 grid, one can observe that the speedup always increases as more machines are added. However, the worst results were obtained with configurations that concentrates all processes in the same machine. Recall that the best result for executions with four processes was obtained when four machines are used, and the worst result was obtained when only one machine was used. The same has occurred with eight processes: the best result was obtained in a configuration that distributed the processes across four machines (all machines that we have available). This behavior could be explained by a memory contention: the greater the number of processes running on the same machine, the greater is the memory contention. This can be explained by the internal CPU architecture: the Quad-Core processor that was used in the experiments has only one internal bus connecting the four cores to the main memory.

For the 1001x1001 grid, a slight different behavior was observed. For the execution using four processes, the best configuration was the one involving two, and not four, machines. Probably the communication overhead using four machines exceeded the memory contention observed on the execution using two machines. However, again the worst result was obtained when only one machine was used. The execution with eight processes obtained its best result when four machines were used: the speedup is almost the double of the one obtained with

two machines. This results reinforces the suspicion that the cause of the poor performance obtained when using four cores in the same machine is the memory contention.

All executions involving sixteeen processes obtained poor performance numbers. Again, a possible cause is the memory contention, because in this case all cores in all machines are occupied.

The poor performance possibly caused by memory contention, as referred to several times during this section, has motivated us to perform a more detailed study of this problem. Thus, some additional tests were run aiming to confirm the existence of memory contention in the parallel environment used.

7.2 Memory Contention

To verify if the simultaneous memory access by distinct cores affect the application performance, we performed a small test. Many instances of our sequential simulator were launched on the same computer at the same time. First, a single IMPES instance was executed; then two instances were simultaneously launched and executed; and then three and four instances, respectively. Table 4 presents the results.

Table 4. Simultaneous Execution - IMPES

# instances	1	2	3	4
101x101	0,29	0,29	0,36	0,43
401x401	32	43	63	86
1001x1001	246	315	438	616

The numbers in Table 4 suggest that, in fact, if all processors cores are simultaneously running tasks, the application performance could be hurt.

To confirm the hypothesis that the memory contention is responsible for poor performance or scalability problems, we decide to develop two simple sequential codes.

The first one is represented by the algorithm 1. Again, we executed one, two, three and four instances of this code in one machine.

```
begin
    double k;
    for (i = 0; i < 1000000; i++) do
        for (j = 0; j < 1000000; j++) do
            k = 1/i + 1/j;
        end
    end
end
```

Algorithm 1. Algorithm without memory access

Table 5. Simultaneous Execution - loop without memory access

# instances	1	2	3	4
loop	65,46	65,47	65,50	65,49

This algorithm does not access memory and, as we can see in Table 5, an increase in the number of concurrent instances executed do not impact its performance.

The second algorithm is represented by code 2, executed in the same way that the previously one.

```
begin
    float k[10000][10000];
    for (i = 0; i < 10000; i++) do
        for (j = 0; j < 10000; j++) do
            k[i * j/10][j] = (float)(i + 1.3)/(j + 1.5) + (i + 1.7) * (j + 1.9);
        end
    end
end
```

Algorithm 2. Algorithm with memory access

Table 6. Simultaneous Execution - loop with memory access

# instances	1	2	3	4
loop	32,95	47,82	70,35	105,05

This code, differently to the first one, makes extensive memory access. As can be noticed in Table 6, the execution times increases as more instances of the code are executed simultaneously, thus confirming our suspicious that the memory contention is the primary cause of loss of performance observed in our simulator. Since our simulator constantly accesses the memory, we can conclude that the hardware was responsible for hurting the simulator performance.

8 Conclusions

In this work we described the development and parallelization of a simulator of petroleum reservoirs. The results obtained by the parallel version, for small grid blocks, was not good enough to justify its parallelization. However, for medium grid blocks, a significant improvement in the speedup was observed, which justifies its parallelization. On large grids, we could observe an excellent scalability for the resolution of the saturation equation, and superlinear speedups were obtained.

Analyzing the obtained results, we could observe the occurrence of a memory contention when more than one core in the same machine was used simultaneously. The result of an extended anaysis that involved the development of additional codes and performance of new experiments further contributed to the suggestion that the memory contention was the main responsible for the poor performance observed in some configurations, specially when four cores were used simultaneously.

As future works, we propose the extension of the analysis presented in this work for different types of multiprocessor architectures, such as Intel i7 [16] and AMD Opteron [9] processors. The internal architecture of these processors are quite different from the Core 2 Quad processor. So we believe that the memory contention problems observed in this work might be reduced.

Acknowledgment

The authors thank PETROBRAS, FAPEMIG, UFJF and CNPq for the financial support. We also would like to thank Gustavo Miranda Teixeira for his valuable help.

References

1. Versteeg, H., Malalasekra, W.: An Introduction to Computational Fluid Dynamics: The Finite Volume Method, 2nd edn. Prentice Hall, Harlow (2007)
2. Chen, Z., Huan, G., Li, B.: An improved IMPES method for two-phase flow in porous media. Transport in Porous Media 32, 261–276 (2004)
3. Balay, S., Buschelman, K., Gropp, W.D., et al.: PETSc users manual. Technical Report ANL-95/11, Argonne National Laboratory (2002)
4. Geist, G., Sunderam, V.: Network-Based Concurrent Computing on the PVM System. Concurrency: Practice and Experience 4(4), 293–311 (1992)
5. Message Passing Interface Forum: MPI, a message-passing interface standard. Oregon Graduate Institute School of Science & Engineering (1994)
6. Chen, Z.: Reservoir Simulation: Mathematical Techniques in Oil Recovery. Society for Industrial and Applied Mathematics (2007)
7. Alam, S.R., Barrett, R.F., Kuehn, J.A., Roth, P.C., Vetter, J.S.: Characterization of scientific workloads on systems with multi-core processors. In: IEEE International Symposium on Workload Characterization, pp. 225–236 (2008)
8. Almasi, G.S., Gottlieb, A.: Highly Parallel Computing. The Benjamin/Cummings Publishing Company, Inc., Redwood City (1989)
9. AMD. Processador amd opteron six-core, http://sites.amd.com/us/atwork/promo/Pages/six-core-opteron.aspx (last access November 30, 2009)
10. Aziz, K., Settari, A.: Petroleum Reservoir Simulation. Applied Science Publishers, London (1979)
11. Brown, S., Rose, J.: Architecture of fpgas and cplds: A tutorial. IEEE Design and Test of Computers 13(2), 42–57 (1996)

12. Chai, L., Gao, Q., Panda, D.K.: Understanding the impact of multi-core architecture in cluster computing: A case study with intel dual-core system. In: Seventh IEEE International Symposium on Cluster Computing and the Grid, CCGRID 2007, pp. 471–478 (2007)
13. Curtis-Maury, M., Ding, X., Antonopoulos, C.D., Nikolopoulos, D.S.: An evaluation of openmp on current and emerging multithreaded processors. In: Mueller, M.S., Chapman, B.M., de Supinski, B.R., Malony, A.D., Voss, M. (eds.) IWOMP 2005 and IWOMP 2006. LNCS, vol. 4315, pp. 133–142. Springer, Heidelberg (2008)
14. Duncan, R.: A survey of parallel computer architectures. IEEE Computer Society Press 23(2), 5–16 (1990)
15. Fox, G., Gannon, D.: Computational grids. Computing in Science and Engineering 3(4), 74–77 (2001)
16. Intel. Processador intel core i7, http://www.intel.com/products/processor/corei7EE/index.htm (last access November 30, 2009)
17. Kassem, J.H.A., Ali, S.M.F., Islam, M.R.: Petroleum Reservoir Simulation: A Basic Approach. Gulf Publishing Company (2006)
18. Koederitz, F.: Lecture Notes on Applied Reservoir Simulation. World Scientific Publishing Company, Singapore (2005)
19. MPI-Forum. Mpi: A message-passing interface standard, http://www.mpi-forum.org/ (last access 25 de Agosto de 2009)
20. Pacheco, P.: Parallel Programming with MPI, 1st edn. Morgan Kaufmann, San Francisco (1996)
21. Rosa, A.J., de Souza Carvalho, R., Xavier, J.A.D.: Engenharia de Reservatórios de Petróleo. Interciência, 1st edn (in portuguese)
22. Sloan, J.D.: High Performance Linux Clusters with OSCAR, Rocks, OpenMosix, and MPI. O'Reilly, Sebastopol (2004)
23. Tenenbaum, A.S.: Modern Operating Systems, 3rd edn. Prentice Hall Press, Upper Saddle River (2007)
24. Thomas, J.E.: Fundamentos de Engenharia de Petróleo. Interciência, Rio de Janeiro, 2nd edn (2001) (in portuguese)
25. Vafai, K.: Handbook of Porous Media. Crc Press, Boca Raton (2005)
26. Zhou, Y., Iftode, L., Li, K.: Performance Evaluation of Two Home-Based Lazy Release Consistency Protocols for Shared Virtual Memory Systems. In: Proceedings of the 2nd Symposium on Operating Systems Design and Implementation (October 1996)
27. Keleher, P., Dwarkadas, A., Cox, A., Zwaenepoel, W.: TreadMarks: Distributed Shared Memory on Standard Workstations and Operating Systems. In: Proceedings of the 1994 Winter Usenix Conference, January 1994, pp. 115–131 (1994)

Generating Parallel Random Sequences via Parameterizing EICGs for Heterogeneous Computing Environments

Hongmei Chi[1] and Yanzhao Cao[2]

[1] Department of Computer & Information Sciences, Florida A&M University
Tallahassee, FL 32307-5100, USA
hchi@cis.famu.edu
[2] Department of Mathematic & Statisticss, Auburn University
Auburn, AL 36830, USA
yzc0009@auburn.edu

Abstract. Monte Carlo (MC) simulations are considered to be ideal for parallelization because a large Monte Carlo problem can often be easily broken up into many small, essentially independent, subproblems. Many Monte Carlo applications are suitable for grid computing environments. In such an environment, the number of substreams is not known in advance in the computing task. This is a challenge for generating random sequences by using the traditional splitting method, which is aimed at ways of partitioning the full period of a single sequence into parallel substreams. Explicit inversive congruential generator(EICG)[1] with prime modulus has some very compelling properties for parallel Monte Carlo simulations. EICG is an excellent pseudorandom number generator for parallalizing via parameterizing. This paper describes an implementation of parallel random number sequences by varying a set of different parameters instead of splitting a single random sequence. Comparisons with linear and nonlinear generators in the library: SPRNG[2] are presented.

Keywords: Grid computing, random number generation, explicit inversive congruential generator, Monte Carlo methods, parameterization, GPU.

1 Introduction

The success of parallel Monte Carlo (MC) computations depends greatly on the quality of the parallel random number generators used. Many MC computations can be carried out effectively on heterogeneous clusters, a computational grid, or even on a fairly unreliable and widely distributed computing environment. In such an environment, computers will operate at very different rates, and some may become unavailable during a large computation. The scheme for parallel random streams we present in this paper provides random numbers for parallel MC simulation without knowing in advance the number of processors needed for the computing task. In addition, this scheme can run a MC simulation on

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 409–417, 2010.

an unreliable computing environment and allow us to compile the overall results only from the computations of these processors that did not fail. Thus, this scheme is suitable for a distributed or grid computing environment [3] and GPU.

Eddy[4] points out that the current various techniques for parallelizing Linear Congruential Generators (LCGs) are not satisfying all of his three requirements for parallel pseudorandom number generators. Alternatively, nonlinear RNGs provide a way to produce high-quality parallel random sequences. Nonlinear congruential method for generating random sequences gives us more promising properties for generating unlimited parallel streams for distributed or grid computing environments [5], which contains various computing units. In such environment, Monte Carlo simulations will consumed thousands, even millions, of random number streams. This is a challenge for generating random sequences by using traditional splitting method, which is aimed at ways of partitioning the full period of a single sequence into parallel substreams.

In the case of explicit inversive congruential generator(EICGs), this means that splitting method concentrates on generating parallel streams from a single sequence from one EICG. In contrast, the scheme described in this paper emphasizes that parallel random streams can be generated with parameterizing different EICGs.

One family of parallelizations of pseudorandom number generators takes a single, long-period, pseudorandom number and splits the full period into subsequences in some manner and the subsequences become the streams for the individual MC processes. However, splitting a single sequence inevitably leads to correlations among the streams that negatively impact "independence" [6]. As a solution to this, one of the authors suggested the use of full-period pseudorandom number generators related to each other through parameterization as an alternative [7,8]. To our best knowledge, there are few papers studying to parallelize EICGs via parameterization. This paper take a closer look at this issue.

A brief description for various parallel methods is presented in §2. §3 will present a discussion of inversive congruential method of generating random numbers. Computing modular inverse is the most costly task in EICGs, therefore we study the current algorithm for modular inversion in §4. §5 briefly described nonlinear generators EICGs and parallelized by parameterization and computational issuse of implementation. It includes some comparisons of the differences between linear methods and nonlinear methods. Conclusions and further work are stated in §6.

2 Methods for Parallel Streams

Many different parallel random number generators have been proposed [9]. Basically, there are the following methods[10] to generate multiple streams for parallel processors.

– Splitting: partitions a single long sequence into subsequences.

- Leap-frog: a single random number sequence is partitioned in turn among the processors as cards are dealt around a card table. If each processor leap-frogs by L in the random number sequence of $\{x_n\}$, processor P_i will generate a random sequence with numbers

$$x_i,\ x_{i+L},\ x_{i+2L}.\ \ldots$$

- Blocking: a single random number sequence is partitioned by splitting it into non-overlapping but contiguous sections. If the length of each section is L in the random number sequence $\{x_n\}$, processor P_i will generate a random sequence with numbers

$$x_{iL},\ x_{iL+1},\ x_{iL+2}.\ \ldots$$

– Parameterization [9,2]: the initial seed or a recurrence parameter of the generator can be carefully chosen in such a way as to produce long period independent sequences on each processor by varying the parameter across processors. For LCGs, the advantage of this scheme is that a full-period LCG sequence is assigned to each processor. Unlike the splitting technique, we do not have to worry about overlapping or exhausting the single parent LCG used in all of the split subsequences.

- Parameterization of an LCG via multiplier [2]: the multiplier, a, in one LCG can be carefully chosen, and each processor is assigned a different multiplier with the same modulus. The ith processor P_i will generate a random sequence with numbers

$$x_n = a_i x_{n-1} \pmod{p}$$

- Parameterization via Modulus [8]: each different LCG will have a different modulus and optimal multiplier assigned to a different processor. The ith processor, P_i, will generate a random sequence with numbers

$$x_n = a_i x_{n-1} \pmod{p_i}$$

Mascagni and Chi [7] described the method of parallelelizing LCGs via parameterizations. This method is successfully applied in SPRNG, which is a package designed for parallel pseudorandom number generators. In this paper, we will give the similar approach of parallelizing EICGs by parameterizing as done in [7]. We consider the scheme for EICG as

$$z_n = (an+b)^{-1} \pmod{p} \tag{1}$$

where $(an+b)^{-1}$ satisfies $(an+b)(an+b)^{-1} = 1 \pmod{p}$ and p is a large prime number.

3 EICGs with Prime Moduli

LCGs are the most commonly used methods for the generation of uniform pseudorandom numbers and have the best developed theory. They are easy to implement and quickly generate pseudorandom numbers. However, LCGs has strong lattice structure, which makes it hard for LCGs to pass Marsaglia's lattice test. Also it suffers long correlation [6] and sensitive to choices of parameter [11]when parallelizing.

Nonlinear congruential methods for the generation of uniform pseudorandom numbers are supplement of linear congruential methods. The nonlinear generators are not producing random streams of a lattice structure. Eichenauer-Herrmann [13] gives a survey on nonlinear methods.

EICGs have desirable statistical independence properties [1]. From discrepancy of sequences of part period and full period, EICGs behave like random numbers. The pseudorandom numbers generated by EICG avoid the planes and instead there are many hyperbolas [14] in the overlapping pair plots.

Also in [15], Marsaglia pointed out that most of linear congruential generators failed the lattice test. Niederreiter [12] proved that EICG pass the Marsaglia's lattice test as long as $s < p/2$, where s is the number of dimensions and p is modulus of (1).

EICGs [12] can produce a large of independent random number sequences as long as parameters a and b of EICGs satisfies some conditions.

Theorem 1. *Consider an EICG,* $z_n^{(i)} = (a_i n + b_i)^{-1} \pmod p$ *with* $a_1, ..., a_s$, *and* $b_1, ..., b_s \in Z_p$ *with* $a \neq 0$ *for* $1 \leq i \leq s$ *If* $b_1 a_1^{-1}$,$b_2 a_2^{-1}$, ..., $b_s a_s^{-1} \in Z_p$ *are distinct, then every hyperpalne in* Z_p^s *contains at most* s *of the points* $(z_n^{(1)}, ..., z_n^{(s)})$.

There are three advantages to for us to consider EICGs for parallelizing via parameterization:

- Not sensitive to selecting parameters.
- Relatively small-size modulus by parameterization.
- Theory support for parallelizing via parameterization [12].

Although EICGs have excellent splitting properties [16], the splitting methods require a long generator period, i.e. a very large modulus has to be chosen. But for computing modular inverse, the larger the modulus, the more computing time required. A large modulus is expensive in the term of computing. On the other hand, parallelization via parameterization needs a medium modulus. Also like LCGs, EICGs are easy to be parameterized as well.

4 Modular Inversion

The most costly computational task of EICG is modular inversion, therefore we must be careful in finding and implementing an efficient algorithm to compute modular inversion.

In general, there are two ways to compute modular inverses: modular exponentiation and extended gcd algorithms[17].

- Modular exponentiation
  The theory of this method is based on Fermat's little theorem [18].

  Theorem 2. *Let p be a prime number. Then any integer, a, satisfies $a^p = a \pmod p$. An integer a that is also not divisible by p will satisfy $a^{p-1} = 1 \pmod p$*

  Since modular inverse of a is defined by $aa^{-1} = 1 \pmod p$, it is easy to see that $a^{-1} = a^{p-2} \pmod p$. Modular exponentiation $a^n \pmod p$ by the repeated squaring method has complexity $O((\log n)(\log^2 p))$, where $n = p-2$. This is larger than the complexity of gcd algorithms.
- Extended gcd algorithm.
  The theory of this method is due to Euclid's gcd algorithm. If $\gcd(a, p) = 1$ and $ax + py = 1$, then $x = a^{-1} \pmod p$. Extended gcd algorithm can compute the multiplicative inverse. Most extended gcd algorithms maintain the current values of x and y as linear combinations of the original x and y and update the values during each iteration. So the extended gcd algorithm will have the same complexity as the gcd algorithm itself.

  $$ax + py = \gcd(a, p) \tag{2}$$

  where x is the inverse of a. Extended Euclid's gcd algorithm gives us the inverse of a.

It is costly computing multiprecision division. There are many algorithms to compute the inverses of multiprecision integers without involving division: binary extended gcd algorithm [19], Lehmer's Euclidean gcd algorithm [20] and Montgomery Modular algorithm [21].

Timing results [20]of variuos modified extended gcd algorithms are given, which shows us that these modified algorithms have not seen significant improvement until the digital sizes of the to given integers are greater than 10^{25}, which means the integers must be greater than 2^{83}. However, we consider the modulus is less than 2^{64}. Therefore, we applied binary extended gcd algorithm as our implementation.

5 Parallelization and Implementation

We implement EICGs as one of pseudorandom number generators of SPRNG. This generator passed both the DIEHARD [22] tests of randomness and the extensive test suite in SPRNG [2]. Detailed implementation is presented as following.

5.1 Parameterization via Multiplier

Parallelizing pseudorandom number generators via parameterization is successfully applied in SPRNG [2]. This method is first proposed via parameterizing LCGs in [9] and extended to general LCG by Mascagni [7,12]. In this paper, the same approach is followed to implement parameterizing EICGs to generate parallel random number sequences.

The theory behind our implementation of EICG is due to the papers by Eichenauer-Herrmann [1] and Niederreiter [12]. Compared to other inversive congruential generators(ICG), EICG is easier to handle in practice. For example, when producing independent substreams, the cost for computations is slightly smaller. We choose a prime number, p, a finite field $Z_p = \{0, 1, ..., p-1\}$ with order of p, a multiplier $a \in Z_p$ with $a \neq 0$, an additive term $b \in Z_p$, and an initial value $n_0 \in Z_p$. Then

$$z_n = (a(n + n_0) + b)^{-1} \pmod{p}, n \geq 0, \tag{3}$$

We have chosen to parameterize the multiplier for parallelization. If modulus is kept the same, there are two parameters a and b left in (3). If parameterization via a or b, then the following theorem [12] guarantees that EICGs can produces a large number of independent random number sequences as long as EICGs satisfies one condition. The theorem tells us that the same modulus and $a_i b_i$ are distinct in Z_p, then we can get independent random subsquences.

Theorem 3. *If $b_1 a_1^{-1}, b_2 a_2^{-1}, ..., b_s a_s^{-1} \in Z_p$ are distinct, then the sequences produced by*

$$z_n^{(i)} = (a_i n + b_i)^{-1} \pmod{p} \tag{4}$$

are independent

where s denotes the number of dimensions and $\{a_i, b_i \in Z_p\}_{1 \leq i \leq s}$, then parallel EICGs can be defined by

$$z_n^{(i)} = (a_i(n + n_0) + b_i)^{-1} \pmod{p}, n \geq 0, \tag{5}$$

and the pseudorandom numbers in the interval $[0, 1)^s$ can be obtained by $x_n^{(i)} = \frac{z_n^{(i)}}{p}$.

Niederreiter [12] suggests two choices of a and b

- $a_i = a$ and $b_i = a(i-1) + b$
- $a_i = am$ and $b_i = an_i + b$ for $\gcd(m, p) = 1$ and $0 \leq n_1 < n_2 < ... < n_s < p$

Here, a is fixed and b is parameterized. However, an EICG can be expressed recursively, and if $z_0 = b^{-1} \pmod{p}$, then $z_n = (z_{n-1}^{-1} + a)^{-1} \pmod{p}$ for $n >= 0$. This shows us that parameter b plays the role of an initial value of the generator. So we leave b out and decide to parallelize the EICGs via the parameter a.

Let $a_i = (a + i)$ and $b_i = b$. Since the period of EICG with prime modulus is p and b is same for each generator, $a_i^{-1} b_i' s$ are distinct as long as a_i^{-1} are different. So we have $\frac{p}{2}$ independent streams.

5.2 Modular Multiplication by Addition and Shifts

The costliest computational task when iterating is modular arithmetic, namely, modular inverse and modular multiplication. We are trying to carefully choose the modulus p such that we can reduce the cost.

With a Mersenne prime as modulus, modular multiplication can be implemented by performing the full integer multiplication with only the inclusion of bitwise shifting and integer addition required to accomplish the modular reduction. We extended the operation to Mersenne-like prime, which is a prime that has the form $2^p - k$, where $k < 2^{\frac{p}{2}}$. Then we can use the same techniques in [2]. We have a detail description in [7]

5.3 Comparisons with Other Generators in SPRNG

In SPRNG, we have another nonlinear generator–MLFG The recurrence relation for this sequence of random numbers is given by the following equation:

$$z_n = z_{n-k} z_{n-l} \pmod{p} \tag{6}$$

l and k are called the lags of the generator and parameterization by lags.

All the following comparisons listed in Table 1 are run at a cluster with 32 node, and each node has two AMD Opreron Processor (246 2.00GHz). MLFG has the advantage of being quicker then EICG. Since each random sequence generated by EICG is independent, there is no need to split one sequence created using a large modulus. In comparisons with other linear generators in SPRNG, EICG is a little slower for generating pseudorandom numbers if the same size moduli are used for all generators. However, parallel EICGs offer much larger number of independent streams. In addition, this parallel method does not require knowing the number of processors in advance.

Table 1. Running Times for Generating Random Numbers in MRS(Million Random Number oer Second)

	LCG64	MLFG	EICG
timing	1.3889	2.7027	2.874
modulus	2^{64}	2^{64}	$2^{32} - 5$

6 Conclusions and Future Work

A new scheme for parallel streams via parameterizing EICGs is proposed. The advantage of this scheme is that we can provide independent streams for MC in heterogeneous computing environment. EICG has strong nonlinear property and generate statistical independence parallel streams. It is an alternative method to generate parallel pseudorandom number streams and the good supplement to SPRNG. However, our numerical results are preliminary results, but promisng.

In this paper, we just consider one type of EICG with same prime modulus. EICGs with different moduli can considered so that unlimited number of the independent substreams can be provided. There are EICGs with composite modulus and with 2^p modulus [13]. Implementations and comparisons among these inversive pseudorandom number generators should be made in future.

In addition, This scheme will be suitable for GPU [23] as well. With continuously increased number of cores in combination with a high memory bandwidth, a recent GPU offers incredible resources for general purpose computing. In such computing environment, GPU can speed up Monte Carlo simulation [24]. For many graphics applications, high quality and speed of parallel RNG are requireed. Our scheme is suitable for this requirement. we will test this scheme in various GPU.

Acknowledgments. Y. Cao's research is partially supported by the US Air Force Office for Scientific Research under grant number FA550-07-1- 0154. H. Chi's research is partially supported by the US Air Force Office for Scientific Research under grant number FA550-07-1-0154 and U.S. Department of Education grant P120A090122.

References

1. Eichenauer-Herrmann, J.: Statistical independence of a new class of inversive congruential pseudorandom numbers. Mathematics of Computation 60, 375–384 (1993)
2. Mascangi, M., Svinuasan, A.: Algorithm 806: SPRNG: A scalable library for pseudorandom number generation. ACM Transactions on Mathematical Software 26, 436–461 (2000)
3. Tatebe, O., et al: Grid datafarm architecture for petascale data intensive computing. In: CCGRID 2002: Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 102–110 (2002)
4. Eddy, W.F.: Random number generators for parallel processors. J. Comp. Appl. Math. 31, 63–71 (1990)
5. Kronstadt, E.P.: Peta-scale computing. In: IPDPS 2005: Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2005) - Papers, p. 38. IEEE Computer Society Press, Los Alamitos (2005)
6. DeMatteis, A., Pagnutti, S.: Parallelization of random number generators and long-range correlations. Parallel Computing 15, 155–164 (1990)
7. Mascagni, M., Chi, H.: Parallel linear congruential generators with sophie-germain moduli. Journal of Parallel Computing 30, 1217–1231 (2004)
8. Chi, H., Jones, E.: Parallel random generators for heterogeneous computing environments. IASTED–PDCS, 163–168 (2005)
9. Percus, O., Kalo, M.: Random number gerenators for mimd parallel processors. J. of Par. and Distr. Comput. 6, 477–497 (1989)
10. Panneton, F., L'ecuyer, P., Matsumoto, M.: Improved long-period generators based on linear recurrences modulo 2. ACM Trans. Math. Softw. 32(1), 1–16 (2006)
11. L'Ecuyer, P.: Tables of linear congruential generators of different sizes and good lattice structure. Mathematics of Computation 68(225), 249–260 (1998)
12. Niederreiter, H.: On a new class of pseudorandom numbers for simulation methods. J. Comp. Appl. Math. 56, 159–167 (1994)

13. Eichenauer-Herrmann, J., Herrmann, E., Wegenkittl, S.: A suvey of quadratic and inversive congruential psedurandom numbers. Lecture Notes in Statistics, vol. 127, pp. 66–97 (1998)
14. Wegenkittl, S.: Are there hyperbolas in the scatter plots of inversive congruential pseudorandom numbers? Journal of Computational and Applied Mathematics 95, 117–125 (1998)
15. Marsaglia, G.: The structure of linear congruential sequences. In: Applications of Number Theory to Numerical Analysis, pp. 249–285. Academic Press, New York (1972)
16. Entacher, K., Uhl, A., Wegenkittl, S.: Linear and inversive pseudorandom numbers for parallel and distributed simulation. In: Twelfth Workshop on Parallel and Distributed Simultation PADS 1998, Banff, Alberta, Canada, May 26-29, pp. 90–97. IEEE Computer Society, Los Alamitos (1998)
17. Knuth, D.E.: The art of Computer Programming, Seminumerical Algorithms, vol. 2. Addison-Wesley, Reading (1997)
18. Koblitz, N.: A course in number theory and cryptography. Springer, Heidelberg (1987)
19. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
20. Sorenson, J.: An analysis of lehmer's eulidead gcd algorithm. In: Proceedings of the 1995 ACM International Symposium on Symbolic and Algebraic (ISSAC 1995), July 10-12, pp. 254–258 (1995)
21. Savas, E., Koc, C.: The montgomery modular inverse–revisited. IEEE Transactions on Computers 49(7), 763–765 (2000)
22. Marsaglia, M.: The diehard battery of tests of randomness, http://stat.fsu.edu/pub/diehard/
23. Sussman, M., Crutchfield, W., Papakipos, M.: Pseudorandom number generation on the gpu. In: GH 2006: Proceedings of the 21st ACM SIGGRAPH/ EUROGRAPHICS symposium on Graphics hardware, pp. 87–94 (2006)
24. Preis, T., Virnau, P., Paul, W., Schneider, J.: Gpu accelerated monte carlo simulation of the 2d and 3d ising model. J. Comput. Phys. 228(12), 4468–4477 (2009)

Efficient Generation of Gray Codes for Reflectable Languages

Limin Xiang, Kai Cheng*, and Kazuo Ushijima

Faculty of Information Science, Kyushu Sangyo University
3-1 Matsukadai 2-Chome, Higashi-ku, Fukuoka 813-8503, Japan
chengk@is.kyusan-u.ac.jp

Abstract. Y. Li and J. Sawada classified a type of language called a reflectable language [Inform. Process. Lett. 109 (2009) 296-300], and gave a generic recursive algorithm GrayCode to list all strings of length n for any reflectable language in Gray code order. GrayCode runs in O(n) worst-case time per string for any application. Based on Williamson's algorithm for k-ary strings, a generic non-recursive algorithm GenericNext is proposed in this paper to list all strings of length for any reflectable language in Gray code order, but the worst-case time is O(1) per string for all the applications mentioned in Y. Li and J. Sawada's paper.

Keywords: Combinatorial problems, Design of algorithms, Analysis of algorithms.

1 Introduction

Strings (words) of length n from a language can be listed in many different orders. When any two consecutive strings in a list are different in exactly one position, the order is called a Gray code order, and the list is called a Gray code. Gray code is originally referred to a specific ordering of length n binary strings is now generally used for an exhaustive listing of any combinatorial object where each successive object differs by some constant amount.

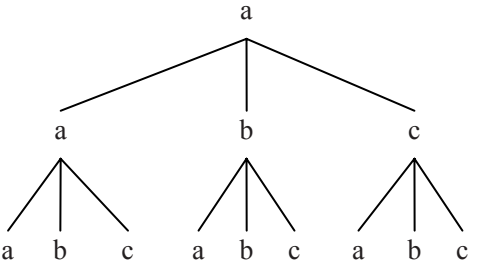
Most Gray code algorithms use a common strategy where reflecting subtrees is applied - a technique that is similar in spirit to the original binary reflected Gray code. Y. Li and J. Sawada [1] has generalized what various representations for combinatorial objects in Gray order have in common by introducing the notion of reflectable languages and proposed a generic recursive Gray code algorithm, called GrayCode .

The straightforward recursive algorithm to generate strings in lexicographic order is by following a computation tree as shown in Fig. 1 (a). In the computation tree, each leaf represents a unique string that is obtained by tracing the path from the root to the leaf. Observe that the resulting listing is not a Gray code since in some cases successive strings may differ in all positions. However, by reflecting (reversing) the order of the children at particular nodes, as illustrated in Fig. 1 (b), a Gray order can be obtained.

* This paper was compiled by Prof. Limin Xiang during his last days. Dr. Xiang passed away on June 2009 after a long battle with cancer. Currently, the corresponding author is Kai Cheng.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 418–426, 2010.

Based on this observation, GrayCode [1] lists all strings of length n for any reflectable language in Gray code order in O(n) worst-case time per string for any application. However, It is not efficient enough for Gray code listing when n is large.



(a) Computation tree for generation lexicographic order

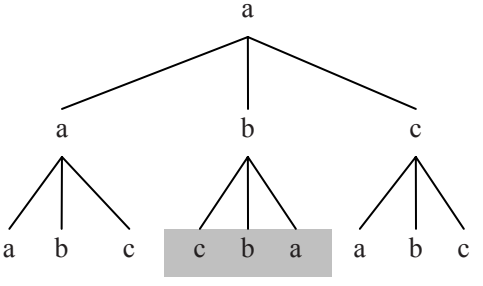


Fig. 1. (b) Computation tree for generating Gray order

In this paper, based on Williamson's algorithm for k-ary strings, a generic non-recursive algorithm, called GenericNext is proposed, which lists all strings of length n for any reflectable language in Gray code order, but the worst-case time is O(1) per string for all the applications mentioned in Y. Li and J. Sawada's paper.

2 Preliminary Definitions

Definition 2.1: A language L over the alphabet Σ is said to be *reflectable* if for every $i > 1$ there exists two distinct characters x_i and y_i in Σ such that if $w_1 w_2 ... w_{i-1}$ is a prefix of a word in L then both $w_1 w_2 ... w_{i-1} x_i$ and $w_1 w_2 ... w_{i-1} y_i$ are also prefixes of words in L.

For easy expression and being understood, some notations are added in Definition 2.2.

Definition 2.2: For a reflectable language L,

(1) x_i and y_i in Definition 1.1 are called *lower* and *upper* reflecting elements at position i, respectively.

(2) if $w_1w_2...w_{i-1}z_i$ is a prefix of a word in L and $z_i \notin \{x_i, y_i\}$, z_i is called a *middle* element of prefix $w_1w_2...w_{i-1}$.

(3) The set is denoted by L_n of all strings with length n for L, and it is assumed that $n \geq 2$ and L_n is nonempty.

A string (e.g., $s_1s_2...s_n$) can be took out from L_n, since L_n is nonempty, and $s_1x_2...x_{n-1}x_n \in L_n$. Let $x_1 = s_1$, and if another character $s'_1 \neq s_1$ is also a prefix of strings in L_n, let $y_1 = s'_1$. Thus, we list all strings of L_n as follows.

1. $x_1x_2...x_{n-1}x_n$ is listed at first, and
2. all the strings in L_n with a common prefix are listed consecutively, such that

   (1) after the strings with prefix $w_1w_2...w_{i-1}a$ ($a \in \{x_i, y_i\}$) are listed, the strings with prefix $w_1w_2...w_{i-1}b$ ($b \notin \{x_i, y_i\}$, if any) are listed, and the strings with prefix $w_1w_2...w_{i-1}c$ ($c \in \{x_i, y_i\} - \{a\}$) are listed last of all.

   (2) after the last one of strings with prefix $w_1w_2...w_{i-1}c$ is listed, the strings with prefix $w_1w_2...w_{i-2}w'_{i-1}c$ ($w'_{i-1} \neq w_{i-1}$, if any) are listed.

Obviously, any two consecutive strings of list above for L_n are different in exactly one position, i.e., the list above is a Gray code for L_n, and it is denoted by $Gc(L_n)$ hereafter. As an example, Fig. 2 gives Gray codes for $L_3 = \{0\} \times \{1,2,3,4\} \times \{5,6,7,8\}$.

Since $x_1\alpha_2...\alpha_{n-1}\alpha_n \in L_n$ ($\alpha_i \in \{x_i, y_i\}$ for $2 \leq i \leq n$), and any $x_1\alpha_2...\alpha_{n-1}\alpha_n$ can be listed as the first string, there are 2^{n-1} Gray codes exist at least for L_n. By changing the order in which the middle elements of a prefix are listed between two reflecting elements at position i for $2 \leq i \leq n$, more Gray codes can be obtained for L_n

In [1], Y. Li and J. Sawada gave a generic recursive algorithm GrayCode to list $Gc(L_n)$. Although any two consecutive strings of $Gc(L_n)$ are different in exactly one position i ($2 \leq i \leq n$), for listing the successor from its predecessor, GrayCode has to recall itself $n-i+1$ times recursively to assign the same value at each position j ($i < j \leq n$). Therefore, GrayCode needs $O(n)$ worst-case time per string. In fact, any recursive Algorithm A needs $O(n)$ worst-case time per string to list strings of L_n (in Gray code order, or, e.g., in lexicographical order), and a non-recursive Algorithm B, obtained by transforming Algorithm A mechanically, needs also $O(n)$ worst-case time per string.

	$Gc_1(L_3)$	$Gc_2(L_3)$	$Gc_3(L_3)$	$Gc_4(L_3)$	$Gc_5(L_3)$	……
1	01[5]	01[5]	01[5]	01[5]	01[8]	
2	016	016	017	017	016	
3	017	017	016	016	017	
4	01[8]	01[8]	01[8]	01[8]	01[5]	
5	02[8]	02[8]	02[8]	02[8]	02[5]	
6	026	027	027	026	026	
7	027	026	026	027	027	
8	02[5]	02[5]	02[5]	02[5]	02[8]	
9	03[5]	03[5]	03[5]	03[5]	03[8]	
10	036	036	036	036	036	
11	037	037	037	037	037	
12	03[8]	03[8]	03[8]	03[8]	03[5]	
13	04[8]	04[8]	04[8]	04[8]	04[5]	
14	046	047	046	047	046	
15	047	046	047	046	047	
16	04[5]	04[5]	04[5]	04[5]	04[8]	

Fig. 2. Gray codes for L_3 ={0}×{1,2,3,4}×{5,6,7,8}

Now that any two consecutive strings of $Gc(L_n)$ are different in exactly one position, it is natural (also more efficient) to list the successor from its predecessor by assigning a new value only at the one position. In Section III, based on Williamson's algorithm Next for k-ary strings [2], a generic non-recursive algorithm GenericNext is proposed to list the successor from its predecessor for $Gc(L_n)$ by assigning a new value only at one position. The worst-case time of algorithm GenericNext is $O(1)$ per string for all the applications mentioned in Y. Li and J. Sawada's paper [1].

3 The Generic Non-recursive Algorithm

Williamson's algorithm for *k*-ary strings [2, p.112] is used to list strings of $S = S_1 \times S_2 \times ... \times S_n$ in Gray code order, where $S_i = \{0,1,...,r_i - 1\}$ ($2 \le r_i \le k$, r_i and k are constants) for $1 \le i \le n$. As mentioned in [1], S is a reflectable language with two reflecting elements 0 and 1 at each position. But in Williamson's algorithm, instead of 1, $r_i - 1$ is the upper reflecting element at position i for

$1 \le i \le n$. Thus, all the middle elements are all the integers between two reflecting elements (i.e., 0 and $r_i - 1$) at position i. In other words, the element can appear at position i in the direction *up* (from 0 up to $r_i - 1$) or in the direction *down* (from $r_i - 1$ down to 0). Let array $v[1..n]$ be used for listing strings of $Gc(S)$ and the upper reflecting element $r_i - 1$ be saved in $r[i]$ for $1 \le i \le n$, Williamson's algorithm can be described as in Figure 2 to generate the next string of $v[1..n]$ for $Gc(S)$, and its idea is described as follows [6].

(1) Two array $e[1..n+1]$ and $d[1..n]$ are employed. Array e is used for keeping track of positions to be processed, and array d is used for indicating the direction (*up* or *down*) for the elements appear at each position between its two reflecting elements.
(2) The first string is with the lower reflecting element at each position (i.e., $v[i] = 0$ for $1 \le i \le n$). Each $e[i]$ $(1 \le i \le n+1)$ and $d[i]$ $(1 \le i \le n)$ are initialized to $i - 1$ and 1 (means *up*), respectively. $e[n+1]$ (the value is n now) supplies the position j to be processed.
(3) The next string of $v[1..n]$ will be obtained by changing the element at position j, i.e., the value of $v[j]$.
    (i) $e[n+1]$ is assigned n.
    (ii) $v[j]$ is assigned $v[j]+1$ if $d[j] = 1$, otherwise $v[j]$ is assigned $v[j]-1$.
    (iii) If the value of $v[j]$ is a reflecting element at position j, then $d[j]$, $e[j+1]$ and $e[j]$ are assigned $1 - d[j]$ (reversing the direction between *up* and *down*), $e[j]$ and j, respectively.
    (iv) j is assigned $e[j+1]$.
(4) When $j = 0$, the last string has been obtained.

For a prefix $W = w_1 w_2 ... w_{i-1}$ of any reflectable language L_n, let Z be the set of all the *middle* elements of W, and $Z' = Z \cup \{x_i, y_i\} = \{z_1, z_2, ..., z_k\}$. Where, $z_1 = x_i$, $z_k = y_i$, and $k \ge 2$. Two functions up and $down$ are defined on Z' as follows.

$up(z_i) = z_{i+1}$ for $1 \le i < k$, and $down(z_i) = z_{i-1}$ for $1 < i \le k$.

Two reflecting elements x_i and y_i are saved in $x[i]$ and $y[i]$, respectively for $1 \le i \le n$. Thus, replacing the statements 2 and 3 in Figure 2, a generic non-recursive algorithm ***GenericNext*** is obtained in Figure 3 to generate the successor from its predecessor for $Gc(L_n)$ by changing the value at only one position.

```
        procedure GenericNext
1         e[n+1] := n
2         if ( d[j] = 1 ) then v[j] := up(v[j]) else v[j] := down(v[j])
3         if (( v[j] = x[j]) or( v[j] = y[j]) )) then
3a          e[j+1] := e[j]
3b          e[j] := j−1
3c          d[j] := 1−d[j]
4         j := e[n+1]
        end
```

Fig. 3. Willamson's algorithm

From Fig. 4, the following theorem holds obviously.

```
        procedure GenericNext
1         e[n+1] := n
2         if ( d[j] = 1 ) then v[j] := up(v[j]) else v[j] := down(v[j])
3         if (( v[j] = x[j]) or( v[j] = y[j]) )) then
3a          e[j+1] := e[j]
3b          e[j] := j−1
3c          d[j] := 1−d[j]
4         j := e[n+1]
        end
```

Fig. 4. Generic non-recursive algorithm

Theorem 3.1: The algorithm ***GenericNext*** runs in $O(1)$ time if functions up and $down$ take $O(1)$ time.

Fortunately, for the applications mentioned in [1], all the up and $down$ functions take $O(1)$ time.

4 Applications

In this section, all the applications mentioned in [1] (except for *open meandric systems,* which will be discussed in another paper) are viewed to show that the time complexity of both up and $down$ functions is $O(1)$ time.

4.1 Binary Strings, *k*-Ary Strings, and Variants

For *k*-ary strings, see Figure 2, function up is $up(v[j]) = v[j]+1$ and function $down$ is $down(v[j]) = v[j]-1$. The same functions up and $down$ above can also be used for binary strings. Furthermore, the algorithm for binary strings can be simplified such as shown in Fig. 5.

```
        procedure NextBinaryString
1         e[n+1] := n
2         v[j] := 1 − v[j]
3a        e[j+1] := e[j]
3b        e[j] := j − 1
4         j := e[n+1]
        end
```

Fig. 5. Next binary string

Strings with a forbidden substring α are a variation on *k*-ary strings. An example in [1] is the language S_3, i.e., the set of all length 3 strings over $\{a,b,c\}$ with no bb substring. S_n will be considered, where, S_n is the set of all length n ($n \geq 2$) strings over $\{a,b,c\}$ with no bb substring. For S_n, *lower* and *upper* reflecting elements are a and c at each position, respectively, function up is

$$up(v[j]) = \begin{cases} b & , \quad (v[j] = a) \wedge ((j = 1) \vee (v[j-1] \neq b)) \\ c & , \quad others \end{cases},$$

and function $down$ is

$$down(v[j]) = \begin{cases} b & , \quad (v[j] = c) \wedge ((j = 1) \vee (v[j-1] \neq b)) \\ a & , \quad others \end{cases}.$$

4.2 Restricted Growth Strings

Restricted growth strings are strings of non-negative integers $(v_1, v_2, ..., v_n)$ satisfying $v_1 = 0$ and $v_j \leq 1 + \max\{v_1, v_2, ..., v_{j-1}\}$ for $1 < j \leq n$. The following discussion is similar to that in [3]. Let $m_j = \max\{v_1, v_2, ..., v_j\}$ for $1 \leq j \leq n$ (saved in

array $m[1..n]$). The *lower* and *upper* reflecting elements are 0 and 1 at each position, respectively. For the restricted growth strings, function up is

$$up(v[j]) = \begin{cases} 1 + m[j-1] & , \quad v[j] = 0 \\ v[j] - 1 & , \quad others \end{cases},$$

and function $down$ is

$$down(v[j]) = \begin{cases} 0 & , \quad v[j] = 1 + m[j-1] \\ v[j] + 1 & , \quad others \end{cases}.$$

After $v[j]$ is renewed, $m[j]$ should be renewed, too. Therefore, the statement $m[j] := new(m[j])$ should be inserted into ***GenericNext*** between statements 2 and 3, where,

$$new(m[j]) = \begin{cases} v[j] & , \quad m[j-1] < v[j] \\ m[j-1] & , \quad others \end{cases}$$

4.3 Binary and k-Ary Trees

Many encoding methods exist for binary and *k*-ary trees [5-8]. Here we only take Zaks' sequences [8] for *k*-ary trees as an example. The set of all the Zaks' sequences for *k*-ary trees with n nodes, denoted by $Z_k(n)$, is (see Theorem 7 in [8])

$Z_k(n) = \{(v_1, v_2, ..., v_n) \mid 1 = v_1 < v_2 < ... < v_n$ and $v_i \le k(i-1)+1$ for $2 \le i \le n\}$

For $Z_k(n)$, the *lower* and *upper* reflecting elements are $k(i-1)+1$ and $k(i-1)$ at position i, respectively for $2 \le i \le n$, function up is

$$up(v[j]) = \begin{cases} v[j-1] + 1 & , \quad v[j] = k(j-1)+1 \\ v[j] + 1 & , \quad others \end{cases},$$

and function $down$ is

$$down(v[j]) = \begin{cases} k(j-1)+1 & , \quad v[j] = v[j-1]+1 \\ v[j] - 1 & , \quad others \end{cases}.$$

In [6], the authors proposed an efficient loopless algorithm to list Gray codes for *k*-ary trees. The algorithm is conceptually simpler than its predecessors. Based on the algorithm, Gray codes for *k*-ary trees with *n* internal nodes ($n \ge 2$ and $k > 3$) can be generated easily.in at least $2^{2(n-1)}$ different ways. The detail can be found in [6] for listing sequences of $Z_k(n)$ in Gray code order.

5 Conclusion

Based on Williamson's algorithm [2, p. 112], a generic non-recursive algorithm ***GenericNext*** was proposed in this paper to list all strings of length n for any reflectable language in Gray code order, and the worst-case time is $O(1)$ per string for all the applications mentioned in [1]. The non-recursive algorithms should exist to list all strings of length n for some non-reflectable languages in Gray code order, also based on Williamson's algorithm. See, for example, the set of combinations of n out of r in the canonical representation [4].

References

1. Li, Y., Sawada, J.: Gray codes for reflectable languages. Information Processing Letters 109, 296–300 (2009)
2. Williamson, S.G.: Combinatorics for Computer Science. Computer Science Press, Rockville (1985)
3. Xiang, L., Cheng, K., Ushijima, K.: On Gray Code for Set Partitions. In: Proc. Information - MFCSIT 2006, Cork, Ireland, August 1-5, pp. 180–183 (2006)
4. Xiang, L., Ushijima, K.: On O(1) Time Algorithms for Combinatorial Generation. The Computer Journal 44(4), 292–302 (2001)
5. Xiang, L., Ushijima, K., Akl, S.G.: Generating regular k-ary trees efficiently. The Computer Journal 43(4), 290–300 (2000)
6. Xiang, L., Ushijima, K., Tang, C.: Efficient loopless generation of Gray codes for *k- ary trees. Information Processing Letters 76, 169–174 (2000)*
7. Xiang, L., Ushijima, K., Tang, C.: Grammar-oriented enumeration of binary trees. The Computer Journal 40(5), 278–291 (1997)
8. Zaks, S.: Lexicographic generation of ordered trees. Theoret. Comp. Sci. 10, 63–82 (1980)

Pattern-Unit Based Regular Expression Matching with Reconfigurable Function Unit

Ming Cong[1], Hong An[1,2], Lu Cao[3], Yuan Liu[3], Peng Li[3], Tao Wang[3], Zhi-hong Yu[3], and Dong Liu[3]

[1] School of Computer Science and Technology,
University of Science and Technology of China, Hefei, 230027, China
[2] Key Laboratory of Computer System and Architecture,
Chinese Academy of Sciences
Beijing, 100190, China
[3] Intel China Research Center
Beijing, 100190, China
mcong@mail.ustc.edu.cn, han@ustc.edu.cn,
{lu.cao,yuan.y.liu,peng.p.li,tao.w.wang,
zhihong.yu,dong.liu}@intel.com

Abstract. Regular Expression (RE) is widely used in many aspects due to its high expressiveness, flexibility and compactness, which requires a high-performance and efficient matching method. A novel approach to accelerate RE pattern matching based on Pattern-Unit (PUREM) is proposed here, in which Pattern-Unit matching is accomplished by a Reconfigurable Function Unit (RFU). The RFU can be integrated into the pipeline of CPU architecture and shares matching jobs with software, without wrecking the compatibility of applications. Compared with other works, our approach offers a flexible mechanism under which hardware does NOT need to vary with RE patterns, and it holds the scalability that can be easily extended to most RE applications and software. For validation, the PUREM HW/SW system has been implemented on the Snort v2.8 and PCRE v7.6 applications. The experimental results show a significant speedup of 3~4x compared to the software performance on a 2GHz Pentium IV machine, where our RFU logic mapped onto Xilinx Virtex-5 XC5VLX50 only takes up 17% resource.

Keywords: Regular expression; Pattern-Unit; Pattern matching; Reconfigurable Function Unit; NFA; DFA.

1 Introduction

Regular expressions (RE) are widely used in many applications such as biomedical, data mining, network processing and etc, and have been studied for decades, due to their expressive power and flexibility for describing useful patterns. Over the years, significant efforts have been made on implementing RE matching in software.

Traditional software technique converts an expression into a Nondeterministic Finite Automaton (NFA) [2,13]. A single regular expression of length n can be expressed as an NFA with $O(n)$ states, as shown in figure 1. In an NFA, more than one

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 427–440, 2010.

state may be active at each step, and the computing complexity for each character of input should be $O(n^2)$ when all n states are active at the same time. A more efficient approach is to convert NFA into Deterministic Finite Automaton (DFA) as shown in figure 2, which has only one active state at a time. DFA is commonly adopted for better suitability for the sequential nature of general purpose processors. However, DFA suffers from state explosion, a theoretical worst case study[1] shows that a DFA representation may generate up to $O(\Sigma^n)$ states where Σ contains the set of input symbols, (i.e. 2^8 from extended ASCII code). Although several studies address the reduction of the required number of states and the improvement of the performance for DFAs in software[11], they are not always applicable and the accuracy of the implementations may be sacrificed.

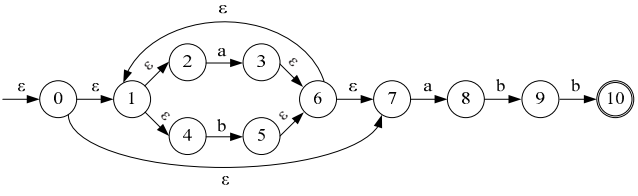


Fig. 1. Example NFA for "*(a|b)*abb*"

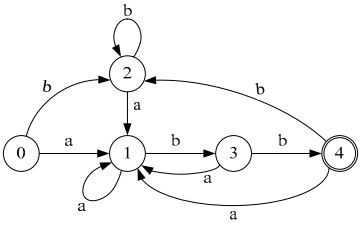


Fig. 2. Example DFA for "*(a|b)*abb*"

The task of searching a collection of data for a pattern set carries out large numbers of independent computations, each of which is matching the input data with only one pattern, so that different pattern matching computations can be assigned into multiple processing elements easily. Since most software platforms for RE matching are based on Von Neumann architecture, the parallelism could not be exploited, the performance does not scale well with the number of RE patterns, and the memory requirements would also be substantially large.

Reconfigurable hardware implementation for RE matching would be a potential approach, such as using FPGAs and etc. Most previous works focus on matching for some specific patterns, which derives high degree of parallelism. Since there is no dependence between the computations, these patterns can be transformed into corresponding circuits which are directly mapped onto FPGA and operate simultaneously. Following the current NFA and DFA theories, many hardware platforms have been proposed for RE matching by implementing DFA/NFA on FPGAs [2,3,4,5,6,7,8]. Although FPGA approach performs much better than that of software-only approach,

hardware platforms still suffer from fixed logics, limited resources and the difficulties of transforming patterns due to the huge numbers of rule sets and the vast differences between them. Any changes on rule sets require recompilation and regeneration of the state automaton, and re-synthesis, re-placement and re-route of the circuits; but it becomes more difficult to fast reconfiguring logics for the given patterns following the fast increasing number of rules.

This paper tries to find a solution to the problems on both the serializability of software and the limited scalability of reconfigurable hardware. A novel Pattern-Unit based Regular Expression Matching(PUREM for short) approach is proposed here. RE patterns are converted into several Pattern-Units, and Pattern-Unit matching is accomplished by a Reconfigurable Function Unit (RFU), which can be integrated into the pipeline of CPU and shares matching jobs with software, without wrecking the compatibility of applications. Furthermore, we validate this approach by implementing on SNORT v2.8 and PCRE v7.6, which shows that our approach is different from the FPGA approach and has unique advantages on the compatibility, resource utilization and flexibility.

In PUREM, a reduced representation of normal NFA is adopted due to its inherent partitionability between both software and RFU. Software partitions REs into sequences of Pattern-Units which can be seemed as atomic units with certain characteristics, and then sends them into RFU for parallel pattern matching at the execution stage, so that the data parallelism can be exploited by increasing comparison granularity from character-level to Pattern-Unit level. From the perspective of hardware, RFU shares matching jobs with software, and only processes the critical matching of Pattern-Units with a sequence of input characters atomically, instead of matching the whole patterns itself, which may lead to unacceptable resource utilization. Moreover, in contrast to previous works on hardware which mostly generate all the circuitry for the given REs, our HW/SW co-operating method, PUREM, benefits from the fact that hardware do not need to vary from the REs sets, and can be easily extended to most other applications and software.

The rest of the paper is organized as follows. Section 2 summarizes the related works. Section 3 gives an overview of PUREM methodology, in which the Patter-Unit and designing of PUREM are introduced consequently. An implementation of PUREM on SNORT is presented in Section 4. The experimental results are discussed in section 5, and Section 6 presents our conclusions and future works.

2 Related Works

The advent of modern reconfigurable hardware technology, particularly FPGAs, has added a new dimension to REs matching. In 2001, Sidhu et al. [2] first noticed that an NFA can be implemented efficiently in hardware. It is shown that for a given RE pattern, each node of its NFA can be implemented as a flip-flop and comparators, logic and routing resources to link the nodes together. Subsequently, Hutchings et al. [3] applied this mechanism to the SNORT rule set, which extracted patterns from different rules in a subset of the SNORT rule database and converted them into a single large RE to generate more general NFA pattern matching circuits. Many works [4,5,6,8] addressed the NFA approach and provided optimization strategies on

resource utilization and performance. Besides, Mitra et al [9] proposed a method to compile PCRE Operation Codes (opcodes) directly into VHDL blocks for parallel implementation on FPGA hardware.

Along with NFA implementations, DFA is another approach for RE matching to be implemented in either hardware or software [10]. Brodie et al [7] developed a hardware structure based on a new and easily pipelined state-machine representation that uses encoding and compression techniques to improve computation density. Kumar et al [11] demonstrated a graph theoretic algorithm to generate D2FA from DFA by combining multiple transitions, which help reduce the memory requirements of DFAs by more than 95%. Compared with NFA implementations, DFA systems tend to take up more resources due to state flattening. However, DFA systems can support dynamic pattern update while NFA can not. Given enough resource in FPGA, those works may get 10-100x speedups over coexistent backtracking-algorithm based software approach in general.

Since software approaches is hard to exploit the inherent parallelism in RE matching, and most previous FPGA-based hardware approaches suffer from generating all corresponding circuits for huge pattern sets, the efficiency is lost and the scalability is limited for pattern matching. Our work address this problem and present a more flexible, scalable and high-performance approach on pattern matching.

3 PUREM Methodology

A HW/SW co-operating approach PUREM for RE matching is proposed, in which software partitions patterns into sequences of predefined Pattern-Units, and then RFU in CPU pipeline matches Pattern-Units with input texts atomically. Therefore, the matching granularity is increased from character by character in original software to Pattern-Unit by Pattern-Unit in RFU, and a potential speedup in performance is expected without wrecking the compatibility of applications.

3.1 Regular Expression

A regular expression or a pattern, is an expression that gives a concise description of a string set. The precise syntax for RE varies not only in context but also among different interpreters. But common formalisms can be extracted to construct REs as following: Literal Characters, Character groups “[ ]”, “[^]”, Alternation “|”, Grouping “( )”and Quantification “?”, “*”, “+”, “{m, n}”.

3.2 Pattern-Unit

Informally, a NFA is a directed graph in which each node is a state and each edge indicates a state transfer and is labeled with a single character or empty character ε. The NFA is not so efficient to implement in software, as the current active state of the NFA may be a set of nodes. Figure 3 shows the corresponding NFA for an example ”*Emails*?*TO*[*u-z*, 0-9]*”.

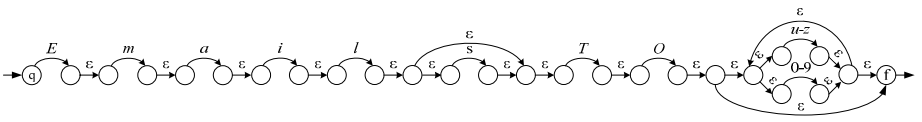


Fig. 3. NFA for "*Emails*?*TO*[*u-z*, 0-9]*"

Based on original NFA definition, we introduce a reduced representation of NFA, as shown in Figure 4. A consecutive sequence of states, which has only one determinate input and output character, is combined into a state, and the driven events between these states are also combined into a character string following the character order in original NFA, such as "*Email*" and "*TO*" in the illustration.

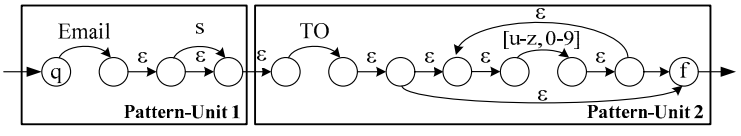


Fig. 4. Pattern-Units division for "*Emails*?*TO*[*u-z*, 0-9]*"

We define the *Pattern-Unit* as a sequence of nodes and edges from the reduced representation of NFA, which can be seemed as an atomic unit and formatted by certain rules. The Pattern-Units might be the pattern formats that appear frequently in pattern rule-sets as well. In this example, we try a more aggressive way for the combination, "*Emails*?", "*TO*[*u-z*, 0-9]*" shown in the box are such Pattern-Units, each of them would be compared in RFU atomically.

This representation may have no benefits for software since it may lead to lots of branches and rollbacks, but with the support of RFU, it can help increase the comparison granularity from character-level to Pattern-Unit level. Without impact the holistic validity and syntax of NFA, we do not need to wreck the algorithms mechanism itself but exploit the potential parallelism in NFA.

3.3 PUREM Design

PUREM is a HW/SW co-operating platform to speedup traditional regular expression matching. In traditional software, the compiler first translates patterns into several opcodes, and then dispatches the corresponding machine instructions to CPU according to these opcodes. While at the stage of compilation in PUREM, Each Patter-Unit is detected and translated into a new corresponding opcode, which is executed by hardware for Pattern-Unit matching. It is obvious that the interface between SW and HW is raised from character comparison to Pattern-Unit matching.

A key point in our PUREM is how to perform Pattern-Unit matching in parallel by hardware. In our approach, Reconfigurable Function Unit (RFU) deals with this problem. The RFU is integrated into the pipeline of processor, which is often called *tightly coupled* mode, and the invoking of RFU should be instruction-based. Therefore the communication costs are relatively small and could be ignored, which may leads to a further speedup in performance.

In this mode, RFU is invoked by special RFU instructions and executes in the way as other instructions such as ALU instructions behave, as shown in figure 5. This configuration is applicable to all the applications. Furthermore, whenever a potential Pattern-Unit is identified for hardware acceleration, we can make it supported by RFU to improve performance. Note that the design of the interface with RFU unit depends on the characteristics of instruction types to be implemented.

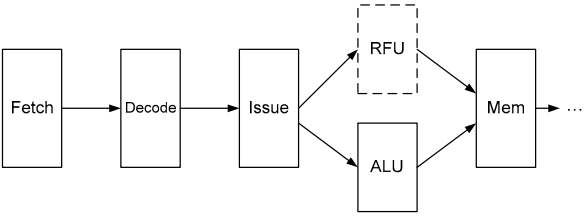


Fig. 5. RFU stage in CPU pipeline

Here only the synchronous in-pipeline RFU is discussed, which has a context and does not have memory access capacity. RFU can store some intermediate results between different execution stages in context, which help eliminate unnecessary data transfers. In this architecture, context registers and control logic are required in RFU for context management. When system context switches, the value in context register inside RFU should also be saved.

RFU is used to accelerate critical parts of the matching process. Whenever a Pattern-Unit appears, RFU is called to process it. Taking RE pattern "*Emails*?*TO*[*u-z*, 0-9]*" for example, as figure 6 shown, it would be partitioned into two Pattern-Units. The first Pattern-Unit is "*Emails*?" in which the prefix part is "*Email*" and the suffix part is "*s*?"; the second is "*TO*[*u-z*, 0-9]*" in which the prefix part is "*TO*" and the suffix part is "[*u-z*, 0-9]*". The two Pattern-Units sent by processor decoder to RFU can be seemed as atom operands. RFU returns result whether it matches and suffix quantifier count to software after comparing each Pattern-Unit with input text. The whole matching process is depicted as figure 6 shows.

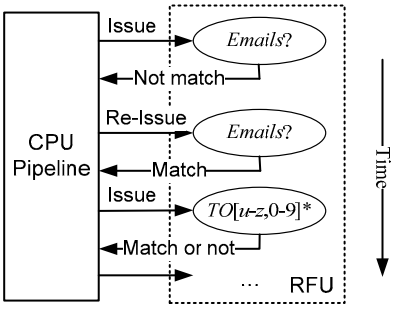


Fig. 6. Matching process for "*Emails*?*TO*[u-z, 0-9]*" on PUREM

Unlike most previous works, our approach is not limited to a certain application or software implementation, and as we known, it is applicable to any RE matching algorithms.

4 PUREM Implementation on SNORT

For a more real and intuitionistic view in this paper, we implement PUREM onto SNORT as a demonstration for validation. SNORT is a popular network intrusion detection system which uses PCRE (Perl Compatible Regular Expression) library for RE matching on payload. While in the PCRE library, each rule is first compiled offline into a special format called *opcode chain*, where an *opcode* corresponds to an operator or normal character in pattern. Next, every generated opcode chain is compared online with every input text line respectively.

4.1 PUREM Design Pattern-Unit selection

This subsection describes how to select Pattern-Units for SNORT application. A statistic on SNORT is studied and classified, and then Pattern-Units for SNORT are listed.

Table 1. Statistics for basic syntaxes supported by regular expressions appeared in SNORT Rule DB 2.8

RE Operator	Occurrences in RE
Anchor: Match the first character "^"	13876 (89.5%)
Anchor: Match the last character"$"	14 (0.1%)
Alternative: "|"	5399 (34.8%)
Priority change: "( )"	5795 (37.4%)
Character Class: "[ ]"	2102 (13.6%)
Negated Character Class: "[^…]"	2006 (12.9%)
Ranged Quantifiers: "{ }"	11574 (74.7%)
Quantifier: "*"	2069 (13.3%)
Quantifier: "+"	1488 (9.6%)
Quantifier: "?"	1281 (8.3%)

Table 1 describes the statistics for basic syntaxes supported by Res, which appeares in SNORT Rule DB 2.8. Both "*" "+" "?" and range "{ }" belong to the type of quantifier; normal characteres, "[ ]"and "[^...]" can be classified into another group of a character set. It shows that a large proportion of the REs in SNORT contain quantifier operators, and a character set often has a quantifier followed behind. So here we restrict the definition of Pattern-Unit to be a combination of signatures of normal characters or character classes with quantifier operators, in which the normal characters or character classes is called prefix characters and the rest is called suffix characters, and they are both optional. Table 2 lists all supported Pattern-Units in our implementation. It is important to note the Pattern-Unit set could be extended as needed.

Table 2. Format of supported Pattern-Unit

-----	Characters + a*	Characters + [ ]*	Characters + [^]*
-----	Characters + a+	Characters + [ ]+	Characters + [^]+
-----	Characters + a?	Characters + [ ]?	Characters + [^]?
Characters	Characters+a{min, max}	Characters+[]{min, max}	Characters+ [^]{min,max}

4.2 PUREM System Implemented on SNORT

At the stage of compilation, the Pattern-Unit combined signatures of normal character or character class with quantifier operators are translated into a new opcode, named as *Superclass*, by the Pattern Formatter in PCRE compiler. While at the stage of execution, RFU would be called by RFU instructions whenever such superclass is captured by software, and the Pattern-Unit matching would be executed atomically. Figure 7 shows the overview of our PUREM HW/SW co-operating system.

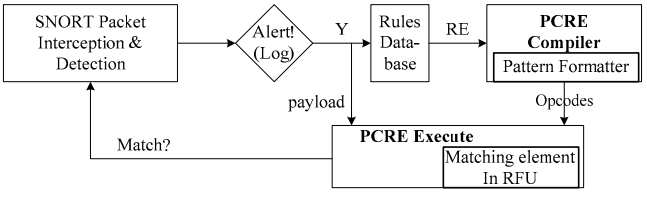


Fig. 7. PUREM system implemented on SNORT

RFU Instructions. The numbers accorded to lemmas, propositions, and theorems, etc. should appear in consecutive order, starting with Lemma 1, and not, for example, with Lemma 11. Since the RFU in this connection is tightly coupled and synchronous, the invoking of RFU should be instruction-based. RFU instructions need to be defined carefully since they form interfaces between software and hardware and should present necessary information as needed. In our implementation, three types of RFU-instructions are introduced as follows, which accords with other instruction formats.

(1) "*RFU_put_context reg1*" is designed to fill context into RFU, in which a Pattern-Unit is encoded in operand *reg1* and sent as the context to RFU. Since a Pattern-Unit may be compared with a sequence of input texts several times, it is effective to keep the input Pattern-Unit as context to reduce communications between hardware and software.

(2) "*RFU_exec1 reg1, reg2*" is used to send input texts which are stored in both *reg1* and *reg2*, while the comparison result is returned by *reg1*. Therefore the length of text data reserved in RFU is up to 32 Bytes, which means the comparison granularity could be increased up to 32-Bytes at a time, and also the number of RFU instructions after compilation is largely reduced.

(3) "*RFU_exec2 reg1, reg2*" is only sent at the end of the text data, in which the lowest byte of *reg2* is used to indicate the end of input text, and the rest of *reg2* and *reg1* are still used for text transfer.

RFU acts differently while distinct instructions come. In a normal operation, the context of RFU is filled by instruction (1), and RFU begins to execute whenever instructions (2) or (3) arrives, and matching for current input texts terminates when instruction (3) is received.

RFU Design in PUREM. The RE matching process in RFU can be partitioned into two stages. The first is a Multiple-character fast-filtering stage, in which RFU engine can fast filter many unmatched texts and move to the position where text that are likely to match, according to the result of comparing parts of pattern with previous input texts. E.g. when a anchor(^) appears at the beginning of pattern, fast-initial-bytes mechanism in this stage would scan 32-Bytes input text with only the initial characters of pattern at a time, which could fast filter unmatched characters in text, while software does it 32 times iteratively.

The second is a general matching stage, in which the RFU engine compares Pattern-Unit with texts in parallel. RFU is invoked by CPU when the RFU-instructions executes. The architecture of RFU design is presented in Figure 8, and details will be described next.

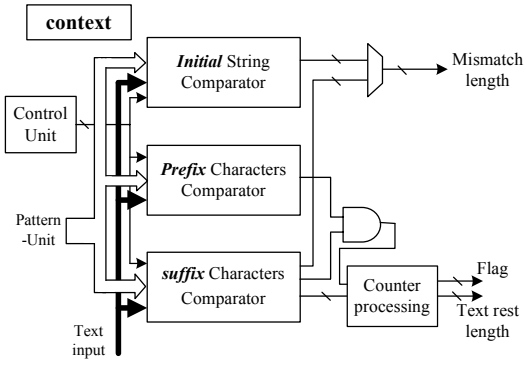


Fig. 8. RFU architecture

Firstly, RFU fetches the Pattern-Unit from "*RFU_put_context*" instrution and puts it into the internal context of RFU. "*RFU_exec1*" or "*RFU_exec2*" instruction invokes RFU. Control Unit in RFU decodes input pattern from instruction operand, breaks up both Pattern-Unit and input text into prefix part and suffix part, according to the length and format information in the pattern, and then dispatches them into "*Prefix* Characters Comparator" and "*Suffix* Characters Comparator" separately.

The "*Initial* String Comparator" works after receiving initial string of the pattern from Control Unit. It scans the whole input text quickly for the first matching position where a possible match may occur. The "Prefix Characters Comparator" compares prefix characters of Pattern-Unit with text only at the start position of text, and returns a Boolean value that indicates whether match happens. The "Suffix Characters Comparator" compares suffix pattern with the suffix part of text, counts suffix characters for the quantifier, and returns the match value and counter value. All these comparators work in parallel. Figure 9 gives a demonstration of the partition method for characters.

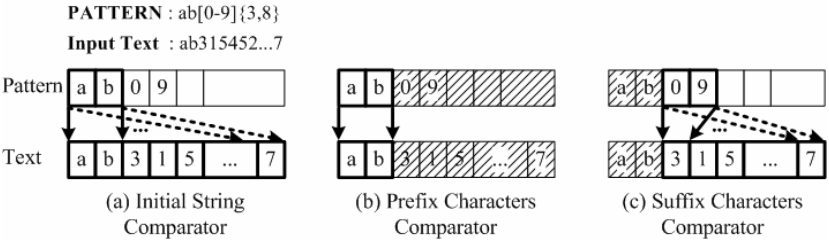


Fig. 9. Function of three comparators. For a giving pattern "*ab*[0-9]{3,8}", (a) the "Initial Sting comparator" compares "*ab*" with characters from the start to the end of text in parallel; (b) "Prefix Characters comparator" only compares "*ab*" with the prefix part of the text;(c) "Suffix Characters comparator" compares [0-9] with characters "315452..7" in the suffix part of the text in parallel.

After that, RFU collects matching result from the output of both "Prefix Characters Comparator" and "Suffix Characters Comparator", and then the "Counter Processing" compares suffix counter with the upper and lower bound of quantifier, it does not return any count value but just the length of left texts after comparison and a "Flag" which announces to software for next expected inputs.

Finally, RFU reserves current count value for quantifier and Pattern-Unit not finished yet into context, it also reserves current matched count range for quantifier {m,n} and determines whether a quantifier loop is ended in comparison, by which overhead caused by the software branches can be greatly reduced. Furthermore, RFU holds Pattern-Unit like […]{m, n} (as mentioned in table 2) in context for the next comparisons if quantifier count in current process does not reach the lower bound value "m".

5 Evaluation Environment

In this section, we present the evaluation environment and methodology of our RE pattern matching design. The baseline software implementations are the latest version of software RE matching tool, including PCRE v7.6 and SNORT v2.8. In the experiment, DARPA Intrusion Detection Data Sets (120MB network data) [Rossey2002], which are the standard corpora for evaluation of computer network intrusion detection systems collected and distributed by MIT Lincoln Laboratory, are matched against all the SNORT rules (2008-04-22 version), which contains 2223 different REs. Dataset used in the experiment is from LLDOS 1.0 - Scenario One in dataset 2000, containing about 120MB network data.

Besides, the RFU designs have been mapped onto Xilinx XC5VLX50 chip. Since the RFU is expected to be integrated into CPU chip, the on-chip resource should be limited, and here the resource utilization constraint is set in LX50: only less than 20% of LUT resource could be utilized, which could be acceptable to map in-pipeline RFU into a processor die.

5.1 Simulation Methodology

In our experiments the PCRE library should be modified to identify Pattern-Units, as illustrated in figure 7. ASIM[12] is used for performance evaluation, which is a software simulator widely used inside Intel. It decouples performance simulation from function simulation. Function simulator uses a pipelined abstract execution engine to insure correctness while performance simulator uses a detailed module specification to achieve cycle-accurate performance simulation. Table 3 shows the parameter of simulated architecture.

Table 3. Parameter of simulated architecture in ASIM

Parameter	Value
Instruction cache size	32KB (4 ways*128 sets*64B)
Data cache size	32KB (8 ways*64 sets*64B)
L2 cache size	256KB(8ways*512 sets*64B)
L2 latency	10 cycles
CPU frequency	2.0GHz
RFU frequency	189.5MHz

5.2 Experimental Results

The performance of our PUREM is compared with Snort v2.8 and PCRE v7.6 (both compiled with GCC "-O3" option) running on a 2GHz Pentium IV processor. The maximum frequency of our RFU implemented on Xilinx Virtex-5 achieves 189.502MHz, and the slice LUTs utilization is 17%, which is much smaller than others in previous works. The latency for returning value that each invoking need is fixed at 4 FPGA cycles (each FPGA cycle equals to 10.6 CPU cycles of Pentium IV in this implementation).

The computation time of PUREM can be partitioned into three parts: the first part remained in CPU core, the second part in RFU and the third part of overhead for CPU to invoke RFU. In our implementation, the tightly coupled RFU executes instructions come from standard CPU instruction flow, and performs just as a function unit in the CPU, so the communication overheads between CPU and RFU are practically small and is neglected.

As the limitation for resource usage, the tradeoff between resources and cycles need to be studied. A decisive factor is the number of bits which compare in parallel. We change the "*RFU_exec"* instructions to send text for different granularity of "fast mismatching" process—1,2,3,4 characters/bytes respectively, and find that a higher filtering proportion is not always the better. The number of "*RFU_exec*" instructions is roughly calculated while 1/2/3/4 characters is used respectively for fast mismatching process, and the results show that instruction numbers are reduced fast from "1" character to "2" characters, but fairly slow afterwards and more resources are utilized at the mean time. Therefore, the width of 2-bytes is chosen as the appropriate granularity for the length of "fast mismatching" in RFU.

The experimental results are illustrated in Figure 10, which shows an average speedup of 3.21x over the match function of PCRE v7.6 called by SNORT v2.8, even

6.7x for some patterns. Our proposed approach is faster than software-based performance in most cases. The speedup derives mainly from the characteristic of high data parallelism in RFU. As described before, up to 32 bytes are compared simultaneously during each execution of RFU while byte by byte comparison is performed in traditional software-based approaches. However, it is also shown that results on some patterns such as NO.31 and NO.33 are below 1. An explanation is that 32-bytes RFU comparison takes more time than original software if the first byte in the string doesn't match.

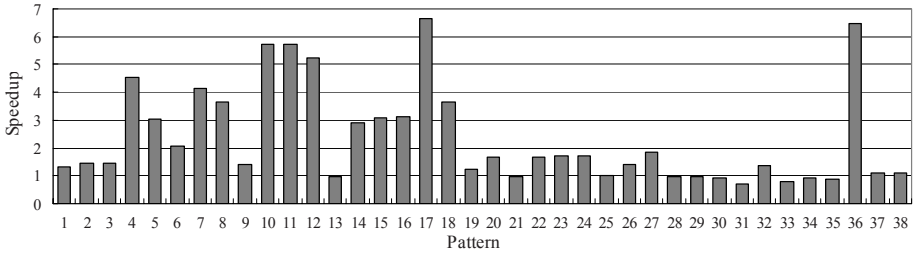


Fig. 10. PUREM Speedup over match function of PCRE 7.6 called by SNORT 2

From the results, we can conclude some key points for implementing PUREM on applications. Firstly, it is obvious that the proportions of the three computation parts in PUREM should be allocated carefully, the part of overhead remained in core should be shrunk, while the effective computation part in RFU increases, which depends on the quality of selected Pattern-Units. Secondly, the communication overheads between the core and the RFU should be reduced by decreasing the instruction counts utilized for RFU. Thirdly, the RFU should provide high CPI while data parallelism is exploited as more as possible, in order to reduce the whole execute time.

Though PUREM implementation on SNORT does not show a high speedup as some previous hardware-based approaches on REs matching, it has some unique advantages on the compatibility, resource utilization and flexibility. Firstly, PUREM methodology has no concern on the software platform chosen by applications, and the semantics of software are still maintained, which ensures full compatibility with applications. Secondly, PUREM approach requires far fewer resources than previous hardware-assist RE systems which may make up full utilization of FPGA chips. Thirdly, with the fast increasing number of REs in each rule sets, PUREM holds the abilities of supporting on-the-fly pattern update and does not need to update while the acceleration engine in traditional hardware approaches must recompile, re-generate the automaton, and re-synthesize, re-placement and re-route the circuits frequently. Lastly, the PUREM methodology can be easily extended to accelerate any kind of SW application that has potential data parallelism, not just for RE matching.

6 Conclusion and Future Work

In this paper, a novel HW/SW co-operating approach to the RE matching called PUREM is proposed, which tries to find a solution to the problems on both the

serializability of software and the limited scalability of reconfigurable hardware methods. Based on a reduced representation of normal NFA, PUREM partitions patterns into sequences of Pattern-Units at the stage of compilation, and then these atomic Pattern-Units are sent into an in-pipeline RFU for matching in parallel at the execution stage. Therefore, the data parallelism can be exploited by increasing comparison granularity from character-level to Pattern-Unit level. In addition, the PUREM approach has unique advantages on the compatibility, resource utilization and flexibility.

We implement PUREM on Snort v2.8 and PCRE v7.6 for validation, the RFU is implemented on a Virtex-5 LX50 at 189.5 MHz and utilizes 17% of the resource in FPGA. Experiment results show an average speedup of 3.21x when compared to a general software PCRE called by SNORT.

For future works, it would be an interesting study to explore different parallel granularity for PUREM, e.g. comparing up to 64Bytes at a time, while meeting the requirements of data width or instructions. We also plan to explore different coupling type for RFU in PUREM, from current tightly coupled to medially coupled type where RFU resides out of CPU chip and communicates by FSB, and evaluate performance improvement at a given communication cost threshold between CPU and RFU.

Acknowledgement(s)

This work is supported financially by the National Basic Research Program of China under contract 2005CB321601,the National Natural Science Foundation of China grants 60633040 and 60970023 and 60736012, the National Hi-tech Research and Development Program of China under contracts 2006AA01A102-5-2 and 2009AA01Z106, the Important National Science & Technology Specific Projects 2009ZX01036-001-002, the China Ministry of Education & Intel Special Research Foundation for Information Technology under contract MOE-INTEL-08-07.

References

1. Hopcroft, J.E., Ullman, J.D.: Introduction to Automata Theory, Languages, and Computation. Addison Wesley, Reading (1979)
2. Sidhu, R., Prasanna, V.K.: Fast RE matching using FPGAs. In: 9th IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 227–238. IEEE Press, Los Alamitos (2001)
3. Hutchings, B.L., Franklin, R., Carver, D.: Assisting network intrusion detection with reconfigurable hardware. In: 10th IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 111–120. IEEE Press, Los Alamitos (2002)
4. Clark, C.R., Schimmel, D.E.: Scalable parallel pattern matching on high speed networks. In: 12th IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 249–257. IEEE Press, Los Alamitos (2004)
5. Sourdis, I., Bispo, J., Cardoso, J.M.P., Vassiliadis, S.: RE Matching in Reconfigurable Hardware. Journal of Signal Processing Systems, 99–121 (October 2007)

6. Cho, Y., Smith, W.H.M.: Deep packet filter with dedicated logic and read only memories. In: 12th IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 125–134. IEEE Press, Los Alamitos (2004)
7. Brodie, B.C., Cytron, R.K., Taylor, D.E.: A Scalable Architecture For High-Throughput Regular-Expression Pattern Matching. In: 33rd Annual International Symposium on Computer Architecture, ISCA 2006, pp. 191–202 (2006)
8. Lin, C.-H., Huang, C.-T., Jiang, C.-P., et al.: Optimization of Pattern Matching Circuits for RE on FPGA. IEEE Transactions on Very Large Scale Integration (VLSI) Systems 15(12), 1303–1310 (2007)
9. Mitra, A., Najjar, W.A., Bhuyan, L.N.: Compiling PCRE to FPGA for accelerating SNORT IDS. In: ACM/IEEE Symposium on Architectures for Networking and Communications Systems, Orlando, pp. 127–136 (2007)
10. Moscola, J., Lockwood, J., Loui, R.P., Pachos, M.: Implementation of a content-scanning module for an internet firewall. In: 11th Field-Programmable Custom Computing Machines, pp. 31–38. IEEE Press, Los Alamitos (2003)
11. Kumar, S., Dharmapurikar, S., Yu, F.: Algorithms to accelerate multiple regular expressions matching for deep packet inspection. In: Proceedings of the SIGCOMM 2006 conference on Applications, technologies, architectures, and protocols for computer communications, October 2006, vol. 36(4), pp. 339–350 (2006)
12. Emer, J., Ahuja, P., Borch, E., et al.: Asim: A performance model framework. Computer 35(2), 68–76 (2002)
13. Hopcroft, J.: An nlogn algorithm for minimizing states in a finite automaton. In: Kohavi, J. (ed.) Theory of Machines and Computation, pp. 189–196. Academic, New York (1971)

Availability Analysis of an IMS-Based VoIP Network System

Toshikazu Uemura[1], Tadashi Dohi[1], and Naoto Kaio[2]

[1] Department of Information Engineering, Graduate School of Engineering
Hiroshima University, 1–4–1 Kagamiyama, Higashi-Hiroshima, 739–8527 Japan
[2] Department of Economic Informatics, Faculty of Economic Sciences
Hiroshima Shudo University, 1–1–1 Ohzukahigashi, Asaminami-ku, Hiroshima, 739–3195, Japan

Abstract. In multimedia wireless networks, VoIP (voice over internet protocol) technology is commonly used to compress the voice information based on a various type of coding techniques, transform it to the packet data, and transmit with real time on IP network. Since the VoIP network is often faced by external threats, a number of security failures may occur at each level of end-user, server and service provider. In this paper we focus on an intrusion tolerant architecture combined an IMS (IP multimedia subsystem), which is a information management middleware developed by IBM Inc., with the VoIP network system. More specifically, we describe the stochastic behavior of the IMS-based VoIP network systems with/without intrusion tolerant mechanism by semi-Markov processes, and evaluate quantitatively their security effects and robustness in terms of both service availability and mean time to security failure.

Keywords: Multimedia service, IMS-based VoIP network, network security, intrusion tolerant system, service availability, mean time to security failure, semi-Markov analysis.

1 Introduction

Intrusion tolerant techniques, inspired from traditional techniques commonly used for tolerating accidental faults in hardware and software systems, have received considerable attentions to complement intrusion avoidance techniques (vulnerability elimination, strong authentication, *etc.*) and to improve the security of systems connected to the Internet [4]. So far, most efforts in security have been focused on specification, design and implementation issues. In fact, several implementation techniques of intrusion tolerance at the architecture level have been developed for real computer-based systems such as distributed systems [3], database systems [9,10], middleware [22,23], server systems [6]. Stroud *et al.* [18] reported the MAFTIA (Malicious and Accidental Fault Tolerance for Internet Applications) project which was a three-year European research project and explored the techniques to build actual intrusion tolerant systems. The above

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 441–456, 2010.

implementation approaches are based on the redundant design at the architecture level on secure software systems. In other words, since these methods can be categorized by a design diversity technique with redundancy in secure system design and need much cost for the development, the effect on implementation has to be evaluated carefully and quantitatively.

The quantitative evaluation of information security based on modeling is becoming much popular to validate the effectiveness of computer-based systems with intrusion tolerance. Littlewood *et al.* [8] discovered the analogy between the information security theory and the traditional reliability theory in assessing the quantitative security of operational software systems, and explored the feasibility of probabilistic quantification on security. Jonsson and Olovsson [7] gave a quantitative method to study the attacker's behavior with the empirical data observed in experiments. Ortalo, Deswarte and Kaaniche [13] applied a privilege graph and a continuous-time Markov chain (CTMC) to evaluate the system vulnerability, and derived the mean effort to security failure. Singh, Cukier and Sanders [16] designed stochastic activity networks model for probabilistic validation of security and performance of several intrusion tolerant architectures. Stevens *et al.* [17] also proposed probabilistic methods to model the DPASA (Designing Protection and Adaptation into a Survivable Architecture).

On the other hand, it would be quite effective to apply the traditional Markov/semi-Markov modeling approaches to design the state transition diagram of system security states by incorporating both attacker's and system behaviors under uncertainty. Madan *et al.* [11,12] dealt with an architecture with intrusion tolerance, called SITAR (Scalable Intrusion Tolerant Architecture) and described the stochastic behavior of the system by a CTMC. They also derived analytically the mean time length to security failure. Uemura and Dohi [19,21] also focused on the typical denial of service (DoS) attacks for a server system and formulated the optimization problems on the optimal patch management policy via continuous-time semi-Markov chain (CTSMC) models. The security evaluation of an intrusion tolerant database (ITDB) system was considered by Yu, Liu and Zang [27] and Wang and Liu [25], who developed simple CTMC models to evaluate the survivability of the ITDB. Recently, this model was extended by the same authors [20] to a CTSMC with a control parameter. The above references concerned the service availability in various real systems from the view points of security and survivability.

In this paper we consider quantitative security evaluation of a VoIP (voice over internet protocol) network system. In multimedia wireless networks, the VoIP technology is commonly used to (i) compress the voice information based on a various type of coding techniques, (ii) transform it to the packet data, and (iii) transmit with real time on IP network. Since the VoIP network is often faced by external threats, a number of security failures may occur at each level of end-user, server and service provider. Bai and Vuong [1], Wu *et al.* [26] and Sengar *et al.* [15] designed intrusion detection architectures for VoIP systems. On the other hand, Chan and Pant [2] and Pant *et al.* [14] focused on an

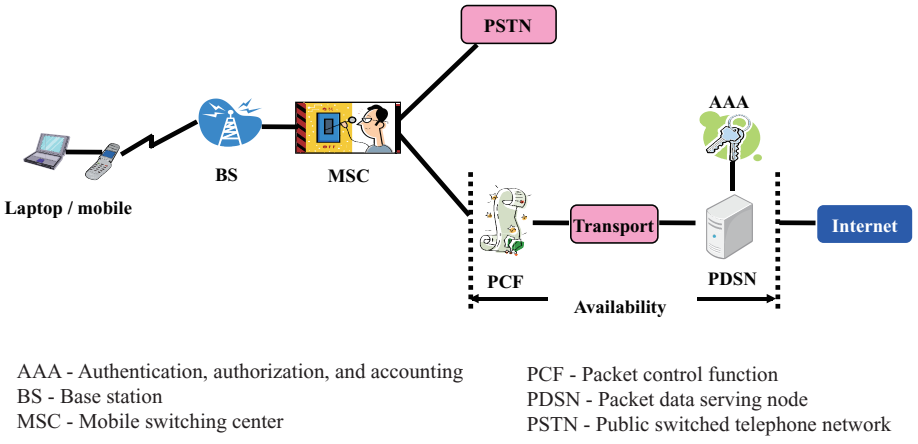


Fig. 1. Configuration of a VoIP network system

intrusion tolerant architecture combined with an IMS (IP multimedia subsystem), which is a information management middleware developed by IBM Inc., with the VoIP network system. Unfortunately, it is worth mentioning that the above references [2,14] gave only the state transition models based on simple CTMCs to qualify the security attribute of the IMS-based VoIP network system. In other words, they did not carry out the quantitative evaluation of security effects by the intrusion tolerant architecture. The essential problem in Pant *et al.* [14] is that the transition from a vulnerability state to an attack/intrusion state is given by an exponential distribution in the CTMC framework. This assumption is not, of course, acceptable because malicious attackers tend to attack as soon as the vulnerable state is detected. Hence our purpose here is to develop a more general CTSMC model to quantify the security of the IMS-based VoIP network system. The basic analysis technique is based on the well-known embedded Markov chain (EMC) approach and is similar to Madan *et al.* [11,12], although our model under consideration is much more complex.

The paper is organized as follows. In Section 2, we introduce the VoIP systems with/without intrusion tolerant mechanism and describe their stochastic behavior by using transition diagrams of CTSMPs. In Section 3 and Section 4, we perform the behavioral analysis of two models and derive the steady-state service availability, which is defined by the probability that the VoIP system can provide a service in the steady state. Numerical examples are devoted in Section 5 to assess the intrusion tolerant effects numerically as well as to examine the sensitivity of model parameters, which govern the operational circumstance of VoIP networks. As mentioned before, since the implementation of intrusion tolerant architectures is very expensive in general, the comparative study by using stochastic models are quite valuable and helpful for quantifying the service availability. Finally, the paper is d in Section 6 with some remarks.

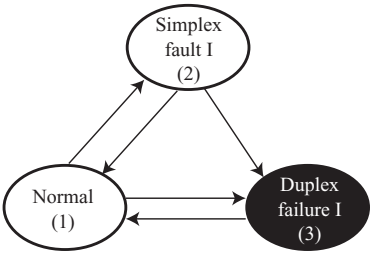


Fig. 2. State transition diagram of a two-unit system without security vulnerability

2 IMS-Based VoIP Network

Voice-over-Internet protocol (VoIP) is a protocol optimized for the transmission of voice through the Internet or other packet-switched networks, and is often used abstractly to refer to the actual transmission of voice. Once the voice information is sent from wireline or wireless endpoints to mobile switching center (MSC) through base station (BS), it can be transmitted into public switched telephone network (PSTN) and IP network separately in accordance with each requirement. Especially, the packet data is sent to packet data servicing node (PDSN) through packet control function, and the authentication, authorization and accounting are checked on PDSN. Figure 1 illustrates a configuration of the VoIP network system. Chan and Pant [2] considered simple CTMC models to analyze a VoIP network system without intrusion tolerance. Further, Pant *et al.* [14] took account of an IP multimedia subsystem (IMS)-based VoIP networks, where the IMS reference architecture fits in an overall converged IP network architecture. To address the potential vulnerabilities in IMS-based VoIP networks, telecommunications service providers can benefit from a comprehensive end-to-end security framework to guide their network planning and the ongoing security assessments performed against their networks. In that sense, the quantitative modeling for IMS-based VoIP networks is quite important even for the service providers.

First of all, we suppose that the network system consists of two operating system (OS) units with redundancy. Figure 2 illustrates a CTMC state transition diagram of the two-unit OS, where one OS is operative but the other one is in stand-by. In this figure, *Normal* (1) means that an OS is operating with a stand-by unit. If the priority task fails on the currently running OS, then it is switched to the stand-by OS and the state goes to *Simplex Fault I* (2) with degradation state. Then the retry operation of the original OS starts immediately under the assumption that the switching is perfect. If the retry is completed without failure, then the originally running OS is put on the stand-by next and the transition to *Normal* (1) occurs. On the other hand, before going to *Normal* (1) if the switching is imperfect, then the system state makes a transition to *Duplex Failure I* (3) and the system is down, where the black color in the figure means

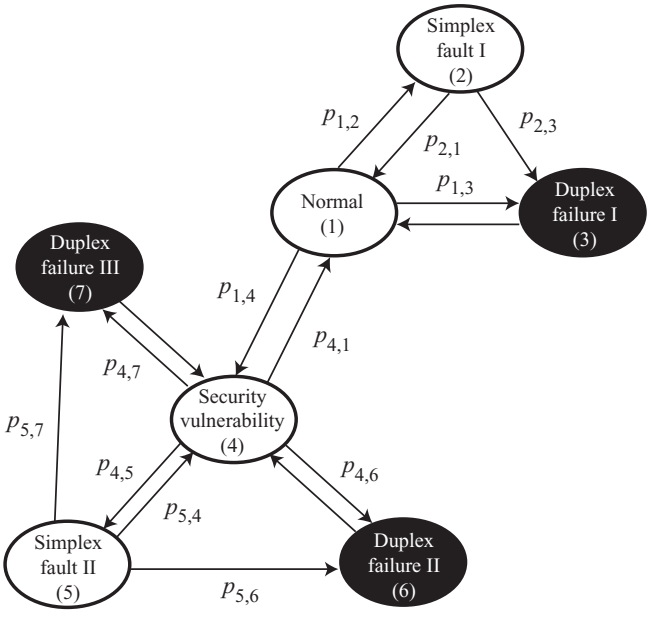


Fig. 3. State transition diagram of a two-unit system with security vulnerability

the system down state. After entering to this state, the retry is triggered for both OSs and the state moves to *Normal* (1) again. The similar cycle repeats again and again for the simple two-unit system model with exponential transitions.

Next, suppose that the system involves security vulnerabilities. In Fig.3, we represent a different CTMC state transition diagram considered by Chan and Pant [2]. If a vulnerability is detected by malicious attackers, then the state goes to *Security Vulnerability* (4), where four possibilities can be considered. If the security patch is ready for the vulnerable part, then the state goes back to *Normal* (1). Since the patch management is not often perfect for an arbitrary vulnerability, the above transition can be skipped for analysis if needed. If the priority task fails but can be switched to the stand-by OS successfully on *Security Vulnerability* (4), then the system state moves to *Simplex Fault II* (5). In Fig.3, *Duplex failure II* (6) and *Duplex Failure III* (7) imply respectively the states where both the priority task and the switching to the stand-by OS fail and where an attack was successful before completing the patch management. Comparing Fig. 2 with Fig.3, it can be seen that the security vulnerability may lead to two possible system down states.

Pant *et al.* [14] further took account of an intrusion tolerant architecture and proposed a more robust design of an IMS-based VoIP network system. Figure 4 depicts the CTMC state transition diagram of the intrusion tolerant VoIP network system. From *Security Vulnerability* (4), the state may go to *Attack* (7) with positive probability, where two possible cases are considered; once an intrusion is detected, the damage by the attack is evaluated through the damage

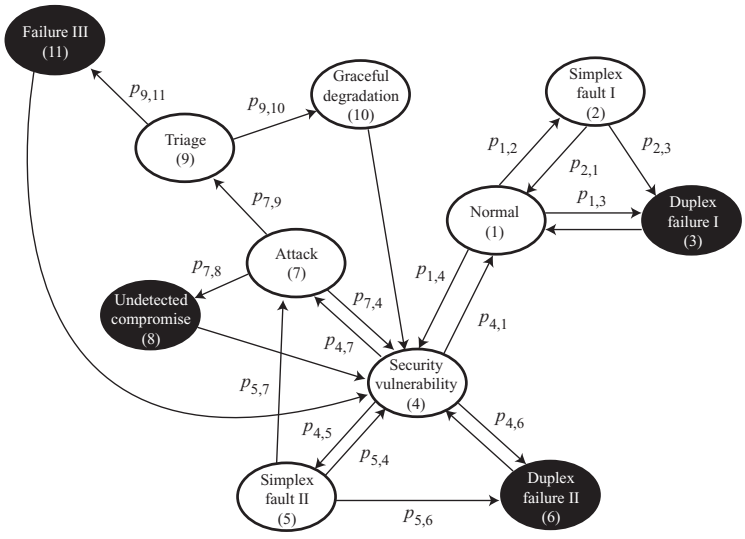


Fig. 4. State transition diagram of a two-unit system with an intrusion tolerant architecture

assessment component. If an effect of the damage is sufficiently small and can be ignored, the damage assessment component judges that it is possible to continue servicing without error, and the detection result of an intrusion can be masked. Then, the state transition occurs from *Attack* (7) to *Security Vulnerability* (4).

When an intrusion cannot be detected, on the other hand, we can further consider two cases; if the attack leads to a serious damage, then the system state goes from *Attack* (7) to *Undetected Compromise* (8). Since in this case the attack is successful and fails to contain the damaged part, it can be regarded as a security failure state. After entering to this state, the damage recovery operation starts immediately and the failure state can be recovered to the vulnerable state again by replacing the destroyed components and recovering the destroyed data. Another possibility is to go to *Triage* (9), where the damage by the attack is assessed timely and is contained. If the damage received is a serious one, then the intrusion tolerance function commands to self-reconfigurate the system, and the state moves to *Failure III* (11) and further to *Security Vulnerability* (4) after completing the recovery operations. Even though the damage does not lead to the security failure, the reconfiguration enables to keep the system state stable. This can be regarded as a fail-secure state, so that the system state goes to *Graceful Degradation* (10) and finally arrives at *Security Vulnerability* (4) in order to continue servicing. In the following discussion, we call two models in Figs. 3 and 4 Model 1 and Model 2, respectively.

In Figs. 3 and 4, let $X_{i,j}$ be the transition time from state i to state j $(i, j \in \{1, 2, \ldots, 11\}$ in the CTSMPs having the c.d.f. $F_{i,j}(t) = \Pr\{X_{i,j} \leq t\}$, the p.d.f $f_{i,j}(t) = dF_{i,j}(t)/dt$ and the mean value $\mu_{i,j} = \mathrm{E}[X_{i,j}]$. Define the hazard rates

for the transition c.d.f. by $r_{i,j}(t) = f_{i,j}(t)/\overline{F}_{i,j}(t)$, where $\overline{F}_{i,j}(\cdot) = 1 - F_{i,j}(\cdot)$ is the survivor functions. If the underlying CTSMCs are ergodic, by taking the limitation of $t \to \infty$, there exist the steady-state probabilities at state $i \in \{1, 2, \ldots, 11\}$ in the CTSMPs, $\pi_i \in [0, 1]$. Similar to Madan *et al.* [11,12], we take the EMC approach for analysis. Consider the embedded discrete-time Markov chains (DTMCs) for the CTSMPs in the steady state. Let $p_{i,j} \in [0, 1]$ denote the steady-state transition probability from state i to state j $(i, j \in \{1, 2, \ldots, 11\})$ in the embedded DTMCs, where we define $p_{1,2} = 1 - p_{1,3} - p_{1,4}$, $p_{2,1} = 1 - p_{2,3}$C$p_{4,1} = 1 - p_{4,5} - p_{4,6} - p_{4,7}Cp_{5,4} = 1 - p_{5,6} - p_{5,7}$, $p_{7,4} = 1 - p_{7,8} - p_{7,9}$ and $p_{9,10} = 1 - p_{9,11}$. Also let h_i be the mean sojourn time at state $i \in \{1, 2, \ldots, 11\}$ in the embedded DTMCs. In thje following sections we analyze two models, Model 1 and Model 2, in Figs. 3 and 4.

3 Analysis in Model 1

3.1 Behavioral Analysis

From Fig.3 in Model 1, it is seen immediately to obtain

$$p_{1,3} = \int_0^\infty \overline{F}_{1,2}(t)\overline{F}_{1,4}(t)dF_{1,3}(t), \tag{1}$$

$$p_{1,4} = \int_0^\infty \overline{F}_{1,2}(t)\overline{F}_{1,3}(t)dF_{1,4}(t), \tag{2}$$

$$p_{2,3} = \int_0^\infty \overline{F}_{2,1}(t)dF_{2,3}(t), \tag{3}$$

$$p_{4,5} = \int_0^\infty \overline{F}_{4,1}(t)\overline{F}_{4,6}(t)\overline{F}_{4,7}(t)dF_{4,5}(t), \tag{4}$$

$$p_{4,6} = \int_0^\infty \overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,7}(t)dF_{4,6}(t), \tag{5}$$

$$p_{4,7} = \int_0^\infty \overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,6}(t)dF_{4,7}(t), \tag{6}$$

$$p_{5,6} = \int_0^\infty \overline{F}_{5,4}(t)\overline{F}_{5,7}(t)dF_{5,6}(t), \tag{7}$$

$$p_{5,7} = \int_0^\infty \overline{F}_{5,4}(t)\overline{F}_{5,6}(t)dF_{5,7}(t) \tag{8}$$

and

$$h_1 = \int_0^\infty t\overline{F}_{1,3}(t)\overline{F}_{1,4}(t)dF_{1,2}(t) + \int_0^\infty t\overline{F}_{1,2}(t)\overline{F}_{1,4}(t)dF_{1,3}(t) + \int_0^\infty t\overline{F}_{1,2}(t)\overline{F}_{1,3}(t)dF_{1,4}(t), \tag{9}$$

$$h_2 = \int_0^\infty t\overline{F}_{2,3}(t)dF_{2,1}(t) + \int_0^\infty t\overline{F}_{2,1}(t)dF_{2,3}(t) \tag{10}$$

$$h_3 = \mu_{3,1}, \tag{11}$$

$$h_4 = \int_0^\infty t\overline{F}_{4,5}(t)\overline{F}_{4,6}(t)\overline{F}_{4,7}(t)dF_{4,1}(t) + \int_0^\infty t\overline{F}_{4,1}(t)\overline{F}_{4,6}(t)\overline{F}_{4,7}(t)dF_{4,5}(t) + \int_0^\infty t\overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,7}(t)dF_{4,6}(t) + \int_0^\infty t\overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,6}(t)dF_{4,7}(t), \tag{12}$$

$$h_5 = \int_0^\infty t\overline{F}_{5,6}(t)\overline{F}_{5,7}(t)dF_{5,4}(t) + \int_0^\infty t\overline{F}_{5,4}(t)\overline{F}_{5,7}(t)dF_{5,6}(t) + \int_0^\infty t\overline{F}_{5,4}(t)\overline{F}_{5,6}(t)dF_{5,7}(t), \tag{13}$$

$$h_6 = \mu_{6,4}, \tag{14}$$

$$h_7 = \mu_{7,4}. \tag{15}$$

3.2 Steady-State Service Availability

By using the mean sojourn times at state $i \in \{1, 2, \ldots, 7\}$, h_i, and the steady-state probabilities $p_{i,j}$ $(i, j) \in \{1, 2, \ldots, 7\}$ in the embedded DTMC in Fig.3, we can derive the steady-state probabilities π_i for the corresponding CTSMC in the following:

$$\pi_1 = h_1/\phi_1, \tag{16}$$

$$\pi_2 = p_{1,2}h_2/\phi_1, \tag{17}$$

$$\pi_3 = (p_{1,3} + p_{1,2}p_{2,3})h_3/\phi_1, \tag{18}$$

$$\pi_4 = \frac{p_{1,4}h_4}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_1}, \tag{19}$$

$$\pi_5 = \frac{p_{4,5}h_5}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_1}, \tag{20}$$

$$\pi_6 = \frac{p_{1,4}(p_{4,6} + p_{4,5}p_{5,6})h_6}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_1}, \tag{21}$$

$$\pi_7 = \frac{p_{1,4}(p_{4,7} + p_{4,5}p_{5,7})h_7}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_1}, \tag{22}$$

where

$$\phi_1 = h_1 + p_{1,2}h_2 + (p_{1,3} + p_{1,2}p_{2,3})h_3 + \frac{1}{1 - p_{4,5} - p_{4,6} - p_{4,7}}\Big\{p_{1,4}h_4 + p_{1,4}p_{4,5}h_5 + p_{1,4}(p_{4,6} + p_{4,5}p_{5,6})h_6 + p_{1,4}(p_{4,7} + p_{4,5}p_{5,7})h_7\Big\}. \tag{23}$$

The steady-state service availability is defined as a fraction of time when the service by the VoIP system can be provided continuously. Hence, the formulation of the steady-state service availability is reduced to the derivation of the mean sojourn time at each state. Note that the service down states correspond to states 3, 6, and 7, so that the steady-state service availability is represented as a function by

$$AV_1 = \pi_1 + \pi_2 + \pi_4 + \pi_5. \tag{24}$$

4 Analysis in Model 2

4.1 Behavioral Analysis

Next we consider Model 2 by taking account of an intrusion tolerant architecture. From Fig.4 we obtain

$$p_{1,3} = \int_0^\infty \overline{F}_{1,2}(t)\overline{F}_{1,4}(t)dF_{1,3}(t), \tag{25}$$

$$p_{1,4} = \int_0^\infty \overline{F}_{1,2}(t)\overline{F}_{1,3}(t)dF_{1,4}(t), \tag{26}$$

$$p_{2,3} = \int_0^\infty \overline{F}_{2,1}(t)dF_{2,3}(t), \tag{27}$$

$$p_{4,5} = \int_0^\infty \overline{F}_{4,1}(t)\overline{F}_{4,6}(t)\overline{F}_{4,7}(t)dF_{4,5}(t), \tag{28}$$

$$p_{4,6} = \int_0^\infty \overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,7}(t)dF_{4,6}(t), \tag{29}$$

$$p_{4,7} = \int_0^\infty \overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,6}(t)dF_{4,7}(t), \tag{30}$$

$$p_{5,6} = \int_0^\infty \overline{F}_{5,4}(t)\overline{F}_{5,7}(t)dF_{5,6}(t), \tag{31}$$

$$p_{5,7} = \int_0^\infty \overline{F}_{5,4}(t)\overline{F}_{5,6}(t)dF_{5,7}(t), \tag{32}$$

$$p_{7,8} = \int_0^\infty \overline{F}_{7,4}(t)\overline{F}_{7,9}(t)dF_{7,8}(t), \tag{33}$$

$$p_{7,9} = \int_0^\infty \overline{F}_{7,4}(t)\overline{F}_{7,8}(t)dF_{7,9}(t), \tag{34}$$

$$p_{9,11} = \int_0^\infty \overline{F}_{9,10}(t)dF_{9,11}(t) \tag{35}$$

and

$$h_1 = \int_0^\infty t\overline{F}_{1,3}(t)\overline{F}_{1,4}(t)dF_{1,2}(t) + \int_0^\infty t\overline{F}_{1,2}(t)\overline{F}_{1,4}(t)dF_{1,3}(t) + \int_0^\infty t\overline{F}_{1,2}(t)\overline{F}_{1,3}(t)dF_{1,4}(t), \tag{36}$$

$$h_2 = \int_0^\infty t\overline{F}_{2,3}(t)dF_{2,1}(t) + \int_0^\infty t\overline{F}_{2,1}(t)dF_{2,3}(t) \tag{37}$$

$$h_3 = \mu_{3,1}, \tag{38}$$

$$h_4 = \int_0^\infty t\overline{F}_{4,5}(t)\overline{F}_{4,6}(t)\overline{F}_{4,7}(t)dF_{4,1}(t) + \int_0^\infty t\overline{F}_{4,1}(t)\overline{F}_{4,6}(t)\overline{F}_{4,7}(t)dF_{4,5}(t) + \int_0^\infty t\overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,7}(t)dF_{4,6}(t) + \int_0^\infty t\overline{F}_{4,1}(t)\overline{F}_{4,5}(t)\overline{F}_{4,6}(t)dF_{4,7}(t), \tag{39}$$

$$h_5 = \int_0^\infty t\overline{F}_{5,6}(t)\overline{F}_{5,7}(t)dF_{5,4}(t) + \int_0^\infty t\overline{F}_{5,4}(t)\overline{F}_{5,7}(t)dF_{5,6}(t) + \int_0^\infty t\overline{F}_{5,4}(t)\overline{F}_{5,6}(t)dF_{5,7}(t), \tag{40}$$

$$h_6 = \mu_{6,4}, \tag{41}$$

$$h_7 = \int_0^\infty t\overline{F}_{7,8}(t)\overline{F}_{7,9}(t)dF_{7,4}(t) + \int_0^\infty t\overline{F}_{7,4}(t)\overline{F}_{7,9}(t)dF_{7,8}(t) + \int_0^\infty t\overline{F}_{7,4}(t)\overline{F}_{7,8}(t)dF_{7,9}(t), \tag{42}$$

$$h_8 = \mu_{8,4}, \tag{43}$$

$$h_9 = \int_0^\infty t\overline{F}_{9,11}(t)dF_{9,10}(t) + \int_0^\infty t\overline{F}_{9,10}(t)dF_{9,11}(t) \tag{44}$$

$$h_{10} = \mu_{10,4}, \tag{45}$$

$$h_{11} = \mu_{11,4}. \tag{46}$$

$$\tag{47}$$

4.2 Steady-State Service Availability

By using the mean sojourn time at state $i \in \{1, 2, \ldots, 11\}$, h_i, and the steady-state probabilities $p_{i,j}$ $(i, j) \in \{1, 2, \ldots, 11\}$ in the embedded DTMC in Fig.**??**, we have

$$\pi_1 = h_1/\phi_2, \tag{48}$$

$$\pi_2 = p_{1,2}h_2/\phi_2, \tag{49}$$

$$\pi_3 = (p_{1,3} + p_{1,2}p_{2,3})h_3/\phi_2, \tag{50}$$

$$\pi_4 = \frac{p_{1,4}h_4}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{51}$$

$$\pi_5 = \frac{p_{1,4}p_{4,5}h_5}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{52}$$

$$\pi_6 = \frac{p_{1,4}(p_{4,6} + p_{4,5}p_{5,6})h_6}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{53}$$

$$\pi_7 = \frac{p_{1,4}(p_{4,7} + p_{4,5}p_{5,7})h_7}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{54}$$

$$\pi_8 = \frac{p_{1,4}p_{7,8}(p_{4,7} + p_{4,5}p_{5,7})h_8}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{55}$$

$$\pi_9 = \frac{p_{1,4}p_{7,9}(p_{4,7} + p_{4,5}p_{5,7})h_9}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{56}$$

$$\pi_{10} = \frac{p_{1,4}p_{7,9}p_{9,10}(p_{4,7} + p_{4,5}p_{5,7})h_{10}}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{57}$$

$$\pi_{11} = \frac{p_{1,4}p_{7,9}p_{9,11}(p_{4,7} + p_{4,5}p_{5,7})h_{11}}{(1 - p_{4,5} - p_{4,6} - p_{4,7})\phi_2}, \tag{58}$$

Table 1. Dependence of parameter (α, κ) on steady-state service availability

(α, κ)	AV_1	AV_2	Δ
(0.2,0.1)	0.4349	0.8086	85.9232
(0.2,0.5)	0.5265	0.8452	60.5195
(0.2,5.)	0.7382	0.9181	24.3744
(0.5,0.1)	0.4812	0.8275	71.9664
(0.5,0.5)	0.6483	0.8889	37.1174
(0.5,5.)	0.8815	0.9600	8.9120
(1.,0.1)	0.5454	0.8523	56.2601
(1.,0.5)	0.7644	0.9262	21.1611
(1.,5.)	0.9511	0.9786	2.8967
(2.,0.1)	0.6404	0.8862	38.3862
(2.,0.5)	0.8723	0.9575	9.7649
(2.,5.)	0.9796	0.9859	0.6443
(5.,0.1)	0.7934	0.9349	17.8364
(5.,0.5)	0.9607	0.9811	2.1248
(5.,5.)	0.9843	0.9871	0.2862

where

$$\begin{aligned}\phi_2 = {} & h_1 + p_{1,2}h_2 + (p_{1,3} + p_{1,2}p_{2,3})h_3 \\ & + \frac{p_{1,4}}{1 - p_{4,5} - p_{4,6} - p_{4,7}}\Big[h_4 + p_{4,5}h_5 + (p_{4,6} + p_{4,5}p_{5,6})h_6 \\ & + (p_{4,7} + p_{4,5}p_{5,7})\Big\{h_7 + p_{7,8}h_8 + p_{7,9}(h_9 + p_{9,10}h_{10} + p_{9,11}h_{11})\Big\}\Big].\end{aligned} \tag{59}$$

Note that the service down states correspond to states 3, 6, 8, and 11, so that the steady-state service availability is represented as a function by

$$AV_2 = \pi_1 + \pi_2 + \pi_4 + \pi_5 + \pi_7 + \pi_9 + \pi_{10}. \tag{60}$$

5 Numerical Examples

Here we investigate effects of the redundant architecture in an intrusion tolerant system by comparing Model 1 with Model 2 from the view points of steady-state service availability. Suppose the following parametric circumstance : $\mu_{1,2} = 30\mathrm{C}\mu_{1,3} = 35\mathrm{C}\mu_{1,4} = 7\mathrm{C}\mu_{2,1} = 1/4\mathrm{C}\mu_{2,3} = 20\mathrm{C}\mu_{3,1} = 5/12\mathrm{C}\mu_{4,1} = 1\mathrm{C}\mu_{4,5} = 20\mathrm{C}\mu_{4,6} = 25\mathrm{C}\mu_{4,7} = 1/2\mathrm{C}\mu_{5,4} = 1/4\mathrm{C}\mu_{5,6} = 10\mathrm{C}\mu_{5,7} = 1/3\mathrm{C}\mu_{6,4} = 1/3\mathrm{C}\mu_{7,8} = 1/3\mathrm{C}\mu_{7,9} = 1/3\mathrm{C}\mu_{8,4} = 1/2\mathrm{C}\mu_{9,10} = 1/4\mathrm{C}\mu_{9,11} = 1/6\mathrm{C}\mu_{10,4} = 5/2$ and $\mu_{11,4} = 1$. For parameter $\mu_{7,4}$, we set $\mu_{7,4} = \mu_{8,4} + \mu_{11,4} = 3/2$ in Model 1 and $\mu_{7,4} = 5/12$ in Model 2.

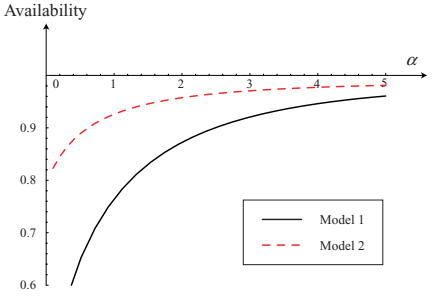


Fig. 5. Steady-state service availability in two models with $\kappa = 1/2$

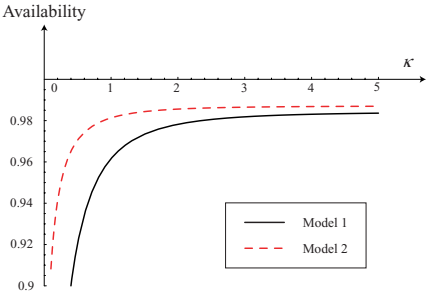


Fig. 6. Steady-state service availability in two models with $\alpha = 3$

5.1 Frequency of Malicious Attacks

Suppose that the p.d.f. $f_{4,7}(t)$ is given by the gamma distribution with shape and scale parameters (α, κ):

$$f_{4,7}(t) = t^{\alpha-1}\frac{\exp\{-t/\kappa\}}{\Gamma(\alpha)\kappa^{\alpha}}, \tag{61}$$

where $\Gamma(\cdot)$ denotes the standard gamma function. The above assumption implies that if $\alpha \leq 1$ ($\alpha \geq 1$) then the time to an attack from the detection point of vulnerability is decreasing (increasing) hazard rate [DHR (IHR)], so that $r_{4,7}(t)$ is decreasing (increasing) in t. Table 1 presents the dependence of the model parameters (α, κ) on the steady-state service availability. In this table, Δ denotes the increment (%) of the steady-state service availability from Model 1 to Model 2, *i.e.*, $\Delta = \{|AV_2 - AV_1| \times 100\}/AV_1$. From this table, it can be seen that the steady-state service availability by adding an intrusion tolerant mechanism could be improved 0.3% at minimum and 85.9% at maximum. This tendency is remarkable in the case where the time to an attack from the detection point of vulnerability is DHR. Also, when κ increases much more, *i.e.*, the time to an attack since the detection of vulnerability is longer, the steady-state service availability monotonically increases.

5.2 Detection Performance

Next we examine the sensitivity of the detection performance in an intrusion tolerant system. Suppose that the p.d.f. $f_{7,9}(t)$ is given by the gamma distribution with shape and scale parameters (β, λ):

$$f_{7,9}(t) = t^{\beta-1}\frac{\exp\{-t/\lambda\}}{\Gamma(\beta)\lambda^{\beta}}. \tag{62}$$

Table 2 presents the dependence of the model parameters (β, λ) on the steady-state service availability. From this table, it can be observed that the steady-state service availability could be improved up to 18.6% $\sim$ 23.1% by adding

Table 2. Dependence of parameter (β, λ) on steady-state service availability

(β, λ)	AV_1	AV_2	Δ
(0.2,0.1)		0.9068	18.6249
(0.2,0.5)		0.9115	19.2402
(0.2,5.)		0.9203	20.3957
(0.5,0.1)		0.9103	19.0866
(0.5,0.5)		0.9201	20.3657
(0.5,5.)		0.9329	22.0415
(1.,0.1)		0.9155	19.7688
(1.,0.5)	0.7644	0.9296	21.6081
(1.,5.)		0.9395	22.9010
(2.,0.1)		0.9237	20.8395
(2.,0.5)		0.9378	22.6863
(2.,5.)		0.9410	23.1022
(5.,0.1)		0.9360	22.4467
(5.,0.5)		0.9410	23.1012
(5.,5.)		0.9411	23.1097

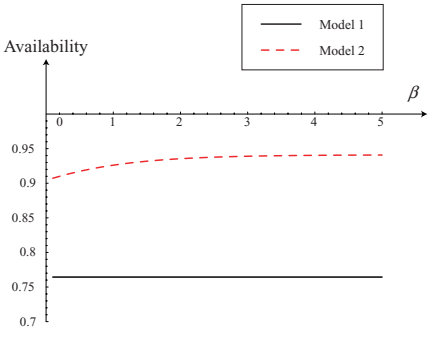


Fig. 7. Steady-state service availability in two models with $\lambda = 1/3$

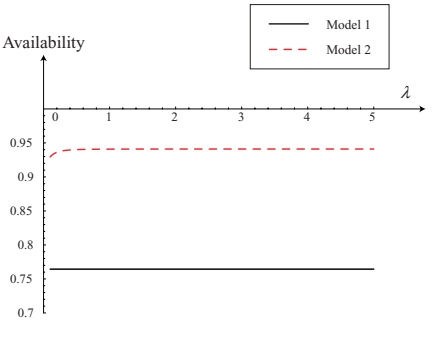


Fig. 8. Steady-state service availability in two models with $\beta = 3$

the intrusion tolerant architecture. This tendency is remarkable in the case where the time to an attack from the detection point of vulnerability is IHR. Also, when κ increases more and more, *i.e.*, the time to an attack since the detection of vulnerability is longer, the steady-state service availability monotonically increases. In [2,14], so that we could obtain a quantitative security evaluation tool for an IMS-based VoIP network.

6 Concluding Remarks

In this paper we have considered an IMS-based VoIP network with an intrusion tolerant architecture, which was a information management middleware developed by IBM Inc., and described the stochastic behavior by semi-Markov

processes. We have evaluated quantitatively the steady-state service availability and compared two models in terms of both frequency of malicious attacks and vulnerability-detection performance. The lesson learned from the numerical examples was that the intrusion tolerant architecture was quite effective to keep the high level of service availability. In the future, we will define other security measures for the VoIP network systems. In addition, when the intrusion tolerant system is developed, a unification of security model and cost model will be needed in considering the tradeoff relation between the expensive development cost and the service level requirement.

Acknowledgments

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (C), Grant No. 19510148 (2007–2008), and the Research Program 2008 under the Center for Academic Development, and Cooperation of the Hiroshima Shudo University, Japan.

References

1. Bai, Y., Vuong, S.: A survey of VoIP intrusions and intrusion detection systems. In: Proceedings of 6th International Conference on Advanced Communication Technology (ICACT 2004), pp. 317–322. IEEE CS Press, Los Alamitos (2004)
2. Chan, C.K., Pant, H.: Reliability and security modeling in upgrading wireless backbone networks. Bell Labs Technical Journal 8(4), 39–53 (2004)
3. Deswarte, Y., Blain, L., Fabre, J.C.: Intrusion tolerance in distributed computing systems. In: Proceedings of 1991 IEEE Symposium on Research in Security and Privacy, pp. 110–121. IEEE CS Press, Los Alamitos (1991)
4. Deswarte, Y., Powell, D.: Internet security: an intrusion torelance approach. Proceedings of the IEEE 94(2), 432–441 (2006)
5. Goseva-Popstojanova, K., Wang, F., Wang, R., Gong, F., Vaidyanathan, K., Trivedi, K., Muthusamy, B.: Characterizing intrusion tolerant systems using a state transition model. In: DARPA Information Survivability Conference and Exposition (DISCEX II), vol. 2, pp. 211–221 (2001)
6. Guputa, V., Lam, V., Ramasamy, H.V., Sanders, W.H., Singh, S.: Dependability and performance evaluation of intrusion-tolerant server architectures. In: de Lemos, R., Weber, T.S., Camargo Jr., J.B. (eds.) LADC 2003. LNCS, vol. 2847, pp. 81–101. Springer, Heidelberg (2003)
7. Jonsson, E., Olovsson, T.: A quantitative model of the security intrusion process based on attacker behavior. IEEE Transactions on Software Engineering 23(4), 235–245 (1997)
8. Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Doboson, J., McDermid, J., Gollmann, D.: Towards operational measures of computer security. Journal of Computer Security 2(2/3), 211–229 (1993)
9. Liu, P.: Architectures for intrusion tolerant database systems. In: Proceedings of 18th Annual Computer Security Applications Conference (ACSAC 2002), pp. 311–320. IEEE CS Press, Los Alamitos (2002)

10. Liu, P., Jing, J., Luenam, P., Wang, Y., Li, L., Ingsriswang, S.: The design and implementation of a self-healing database system. Journal of Intelligent Information Systems 23(3), 247–269 (2004)
11. Madan, B.B., Goseva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S.: Modeling and quantification of security attributes of software systems. In: Proceedings of 32nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2002), pp. 505–514. IEEE CS Press, Los Alamitos (2002)
12. Madan, B.B., Goseva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S.: A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation 56(1/4), 167–186 (2004)
13. Ortalo, R., Deswarte, Y., Kaaniche, M.: Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering 25(5), 633–650 (1999)
14. Pant, H., McGee, A.R., Chandrashekhar, U., Richman, S.H.: Optimal availability and security for IMS-based VoIP networks. Bell Labs Technical Journal 11(3), 211–223 (2006)
15. Sengar, H., Wijesekera, D., Wang, H., Jajodia, S.: VoIP intrusion detection through interacting protocol state machines. In: Proceedings of 36th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2006), pp. 393–402. IEEE CS Press, Los Alamitos (2006)
16. Singh, S., Cukier, M., Sanders, W.H.: Probabilistic validation of an intrusion tolerant replication system. In: Proceedings of 33rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2003), pp. 615–624. IEEE CS Press, Los Alamitos (2003)
17. Stevens, F., Courtney, T., Singh, S., Agbaria, A., Meyer, J.F., Sanders, W.H., Pal, P.: Model-based validation of an intrusion-tolerant information system. In: Proceedings of 23rd IEEE Reliable Distributed Systems Symposium (SRDS 2004), pp. 184–194. IEEE CS Press, Los Alamitos (2004)
18. Stroud, R., Welch, I., Warne, J., Ryan, P.: A qualitative analysis of the intrusion-tolerant capabilities of the MAFTIA architecture. In: Proceedings of 34th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2004), pp. 453–461. IEEE CS Press, Los Alamitos (2004)
19. Uemura, T., Dohi, T.: Quantitative evaluation of intrusion tolerant systems subject to DoS attacks via semi-Markov cost models. In: Denko, M.K., Shih, C.-s., Li, K.-C., Tsao, S.-L., Zeng, Q.-A., Park, S.H., Ko, Y.-B., Hung, S.-H., Park, J.-H. (eds.) EUC-WS 2007. LNCS, vol. 4809, pp. 31–42. Springer, Heidelberg (2007)
20. Uemura, T., Dohi, T.: Optimizing security measures in an intrusion tolerant database system. In: Nanya, T., Maruyama, F., Pataricza, A., Malek, M. (eds.) ISAS 2008. LNCS, vol. 5017, pp. 26–42. Springer, Heidelberg (2008)
21. Uemura, T., Dohi, T.: Optimal security patch management policies maximizing system availability. Journal of Communications (to appear)
22. Verissimo, P.E., Neves, N.F., Correia, M.: Intrusion-tolerant architectures: concepts and design. In: de Lemos, R., Gacek, C., Romanovsky, A. (eds.) Architecting Dependable Systems. LNCS, vol. 2677, pp. 3–36. Springer, Heidelberg (2003)
23. Verissimo, P.E., Neves, N.F., Cachin, C., Poritz, J., Powell, D., Deswarte, Y., Stroud, R., Welch, I.: Intrusion-tolerant middleware. IEEE Security and Privacy 4(4), 54–62 (2006)
24. Wang, F., Gong, F., Sargor, C., Goseva-Popstojanova, K., Trivedi, K., Jou, F.: SITAR: A scalable intrusion-tolerant architecture for distributed services. In: Proceedings of 2nd Annual IEEE Systems, Man and Cybernetics, Information Assurance Workshop, West Point, NY (June 2001)

25. Wang, H., Liu, P.: Modeling and evaluating the survivability of an intrusion tolerant database system. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189, pp. 207–224. Springer, Heidelberg (2006)
26. Wu, Y.-S., Bagchi, S., Garg, S., Singh, N., Tsai, T.: SCIDIVE: a stateful and cross protocol intrusion detection architecture for voice-over-IP environments. In: Proceedings of 34th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2004), pp. 433–442. IEEE CS Press, Los Alamitos (2004)
27. Yu, M., Liu, P., Zang, W.: Self-healing workflow systems under attacks. In: Proceedings of 24th International Conference on Distributed Computing Systems (ICDCS 2004), pp. 418–425. IEEE CS Press, Los Alamitos (2004)

Hybrid Genetic Algorithm for Minimum Dominating Set Problem

Abdel-Rahman Hedar[1] and Rashad Ismail[2]

[1] Dept. of Computer Science, Faculty of Computers and Information, Assiut University, Assiut 71516, Egypt
hedar@aun.edu.eg
[2] Dept. of Mathematics, Faculty of Science, Assiut University, Assiut 71516, Egypt
rashad@aun.edu.eg

Abstract. The minimum dominating set (MDS) problem is one of the central problems of algorithmic graph theory and has numerous applications especially in graph mining. In this paper, we propose a new hybrid method based on genetic algorithm (GA) to solve the MDS problem, called shortly HGA-MDS. The proposed method invokes a new fitness function to effectively measure the solution qualities. The search process in HGA-MDS uses local search and intensification schemes beside the GA search methodology in order to achieve faster performance. Finally, the performance of the HGA-MDS is compared with the standard GA. The new invoked design elements in HGA-MDS show its promising performance compared with standard GA.

Keywords: Minimum dominating set, Genetic algorithm, Meta-heuristics, Hybrid methods, Graph theory.

1 Introduction

The minimum dominating set (MDS) Problem in graph theory seeks to find a subset of nodes of minimum cardinality with the following property: each node is required to either be in the dominating set, or adjacent to some node in the dominating set. We focus on the question of finding a dominating set of minimum cardinality. The MDS problem is a hard combinatorial problem, classified as NP-Complete [3], and in general cannot be solved exactly in polynomial time. This problem arises in network testing, as well as in wireless communication [19].

Computational Intelligence (CI) tools and their applications have grown rapidly since its inception in the early 1990s of the last century [5,15].CI tools were firstly limited to fuzzy logic, neural networks and evolutionary computing as well as their hybrid methods [20]. Nowadays, the definition of CI tools has been extended to cover many of other machine learning tools [2,5,15]. One of the main CI classes is Genetic algorithms (GAs) which are one of the most efficient CI that have been employed in a wide variety of problems [15]. However, GAs, like other CI, suffer from the slow convergence that brings about

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 457–467, 2010.

the high computational cost. GAs, possibly the most prevalent representative of Evolutionary Computation, were first presented by Holland [14]. Since that time GAs have been successfully applied to a wide range of problems including multimodal function optimization, machine learning, and the evolution of complex structures such as neural networks. An overview of GAs and their implementation in various fields is given by Goldberg [7]. The use of CI to solve the MDS problem captivated many researchers [13,12], and GA has been applied to solve this problem.

In this paper, we propose a hybrid GA-based method, called hybrid genetic algorithm for minimum dominating set (HGA-MDS), to solve the MDS problem. HGA-MDS uses a 0-1 variable representation of solutions in searching for the MDS, and it invokes a new fitness function to measure the solution qualities. Therefore, HGA-MDS invokes intensification search schemes besides the GA search methodology. In order to demonstrate the performance effectiveness of the HGA-MDS in terms of solution quality, we compare its performance with the standard GA, and a HGA-MDS with using a second fitness function. According to this comparison, results show that the proposed method obtained superior results.

The paper is organized as follows. In the next section, we briefly give view to the MDS problem as preliminaries needed throughout the paper. In Section 3, we highlight the main components of HGA-MDS and present its formal algorithm. In Section 4, we report numerical results with HGA-MDS. Finally, the conclusion makes up Section 5.

2 Minimum Dominating Set Problem

We consider the minimum dominating set Problem defined as follows. Given a simple undirected graph $G = (V, E)$, V is the set of nodes (or vertices) and E the set of edges, a dominating set is a subset of nodes $D \subseteq V$ such that for all $u \in V - D$ there exists a $v \in D$ for which $(u, v) \in E$. This means that each node is either a member of the dominating set or it is adjacent to some member of the dominating set. If either one of these conditions is satisfied, the node is said to be *covered*. The MDS problem is that of finding in a graph a dominating set of minimum cardinality. The size of a minimum dominating set in a graph G is called the *domination number* of G and is denoted $\gamma(G)$. The MDS problem is one of the central problems of algorithmic graph theory, having, together with its variants, numerous applications and offering various lines of research [9,4,19]. It is also one of the most difficult problems (we refer the reader to [8] for some recent developments on the complexity of the problem). Moreover, the problem remains difficult in many restricted graph families such as planar [6], bipartite [18], split [16], or graphs of bounded node degree [17]. The books of Haynes et al. give a survey on the rich literature of algorithms and complexity of the MDS problem [9,10]. We are interested in the GA meta-heuristic approaches which provide acceptable solutions to this problem.

3 Hybrid Genetic Algorithm for MDS

In this section, we introduce the detail construction of the HGA-MDS method. First, we describe the components of HGA-MDS, and then state the HGA-MDS algorithm formally.

3.1 Solution Representation

As in the standard GA, population P in HGA-MDS contains a certain number M of solutions. HGA-MDS uses a binary representation for solutions. Therefore, a solution x in P is a 0-1 vector with dimension equal to $|V|$, where $|V|$ is number of nodes in the graph. If a component x_i of x, $i = 1, \ldots, |V|$, has the value 1, then the i-th node of the graph is contained in the node subset represented by solution x. Otherwise, the solution x does not contain the i-th node.

3.2 Fitness Function

The fitness function for the MDS problem needs to differentiate between chromosomes based on the number of nodes covered by a chromosome, and also based on the number of nodes contained in this chromosome. Specifically, the fitness function *fit* invoked in HGA-MDS is shown as follows.

$$fit(x) = \frac{n}{|V|} + \frac{1}{|V|\gamma_x(G)}, \tag{1}$$

where n is the number of nodes covered by solution x, and $\gamma_x(G)$ is the number of nodes contained in x. Fitness function consist of two parts, the first part $n/|V|$, reflects the size of domination on G by x. If x represents a dominating set, then this part is equal to 1. While the second part $1/(|V|\gamma_x(G))$ distinguishes between solutions that have the same values of the first part based on the number of nodes contained in each of them.

3.3 Intensification Schemes

An intelligent search method should invoke a wide exploration mechanism as well as a deep exploitation mechanism. HGA-MDS invokes three mechanisms for intensification. The first intensification mechanism is called *LocalSearch*. In this mechanism, we add or delete some nodes to improve the best solution x^{best} found so far, and this process is repeated n_l times. The formal description of this mechanism is shown in Procedure 1.

Procedure 1. LocalSearch(x^{best})

1. *Repeat the following steps n_l times.*
2. *Set $\tilde{x}^{best} = x^{best}$.*
3. *If* $\text{fit}(\tilde{x}^{best}) \geq 1$, *randomly select a component $\tilde{x}_i^{best}$ with value 1. This selection is inversely proportional to the degree of its corresponding node. Set $\tilde{x}_i^{best} = 0$.*

4. *If* $\text{fit}(\tilde{x}^{best}) < 1$, *randomly select a component* $\tilde{x}_i^{best}$ *with value 0. This selection is proportional to the degree of its corresponding node. Set* $\tilde{x}_i^{best} = 1$.
5. *If* $\text{fit}(\tilde{x}^{best}) > \text{fit}(x^{best})$, *set* $x^{best} = \tilde{x}^{best}$.

HGA-MDS applies another intensification mechanism to refine the best dominating set x^{best} found so far, if exists. This mechanism, called *Filtering*, this mechanism filters the best solution to the MDS problem by eliminating some of unnecessary nodes contained in x^{best}. Actually, *Filtering* scheme tries to reduce the dominating set represented by x^{best} without losing the coverage.

Procedure 2. Filtering(x^{best})

1. *If* $\text{fit}(x^{best}) < 1$, *return.*
2. *Compute the set* $W = \{w_1, \ldots, w_{|W|}\}$ *of all positions of value one in* x^{best}.
3. *Repeat the following steps for* $j = 1, \ldots, |W|$.
3. *Set* $x_{w_j}^{best} = 0$, *and compute the new fitness value.*
4. *Update* x^{best} *if the fitness value is increased.*

The final intensification mechanism is called *Elite Dominating Sets Inspiration*. In the HGA-MDS process of finding the MDS, the best n_{DS} dominating seta which have been visited are saved in a set called *Dominating Sets* (*DS*). A trial solution x^{Core} is define as the intersection of the n_{Core} best dominating sets in *DS*, where n_{Core} is a pre-specified number. If the number of nodes involved in x^{Core} is less than that in x^{best} by at least two, then the zero position in x^{Core} which gives the highest node-degree is updated to be one. This mechanism is continued until the number of nodes involved in x^{Core} becomes less than that in x^{best} by one.

Procedure 3. $[x^{Core}] = \text{EliteInspiration}(\text{DS}, n_{Core})$

1. *If* DS *is empty, then return.*
2. *Set* n_F *equal to the number of nodes involved in* x^{best}, *and set* x^{Core} *equal to the intersection of the* n_{Core} *best dominating sets in* DS.
3. *If* $\sum_{i=1}^{|V|} x_i^{Core} < n_F - 1$, *then go to Step 4. Otherwise, return.*
4. *If* $\text{fit}(x^{Core}) \geq 1$, *then return.*
5. *Update the zero position in* x^{Core} *which gives the highest fitness, and go to Step 3.*

3.4 HGA-MDS Algorithm

HGA-MDS starts with an initial population of individuals generated at random. Each individual in the population represents a trial solution to the MDS problem. The individuals evolve through successive generations. During each generation, each individual in the population is evaluated by using a fitness function *fit* (see Equation (1)) to determine their qualities. HGA-MDS applies Procedure

1 to improve the best solution. In each generation, the population is updated through genetic operators. Good individuals are selected based on the linear ranking selection [1]. HGA-MDS invokes the standard one-point crossover and uniform mutation [11] as well as *LocalSearch* Procedure to update the current population. If a certain number of consecutive generations without improvement is achieved, HGA-MDS invokes Procedure 2 to improve the best dominating set x^{best} obtained so far, if it exists. The search may be terminated if the number of generations exceeds g_{max}, or the number of consecutive generations without improvement exceeds a pre-specified number. Finally, *Elite Dominating Set Inspiration* Procedure is applied as a final intensification mechanism. The main structure is shown in Fig. 1 and the formal algorithm is stated below.

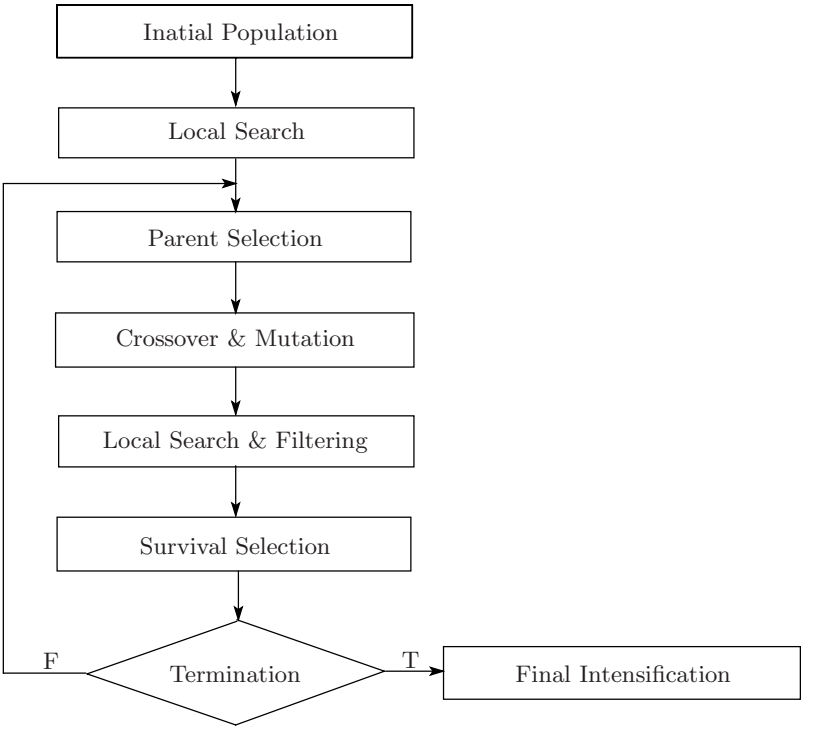


Fig. 1. HGA-MDS Flowchart

Algorithm 4. HGA-MDS

1. ***Initialization.*** *Set values of* M, g_{max}, n_{Core}, n_l. *Set the crossover and mutation probabilities* $p_c \in (0,1)$ *and* $p_m \in (0,1)$, *respectively. set* DS *to be an empty set. Generate an initial population* P_0 *of size* M.

2. ***Local Search.*** *Evaluate the fitness function of all individuals in* P_0 *by using the Equation (1), and then apply Procedures 1 to improve the best trial solution in* P_0*. Set the generation counter* $t := 0$*.*
3. ***Parent Selection.*** *Select an intermediate population* P'_t *from the current population* P_t *using the linear ranking selection [1].*
4. ***Crossover.*** *Apply the standard one-point crossover to chromosomes in* P'_t*, and update* P'_t*.*
5. ***Mutation.*** *Apply the standard uniform mutation to chromosomes in* P'_t*, and update* P'_t*.*
6. ***Survival Selection.*** *Evaluate the fitness function of all generated children in the updated* P'_t*, and set* $P_{t+1} = P'_t$*. If the best solution in* P_{t+1} *is worse than the best solution in* P_t*, then replace the worst solution in* P_{t+1} *by the best solution in* P'_t*.*
7. ***Local Search.*** *Apply Procedure 1 to improve the* x^{best}*, update* DS*.*
8. ***Filtering.*** *If* x^{best} *represents a dominating set, then apply Procedure 2 to improve it, update* DS*.*
9. ***Stopping Condition.*** *If* $t > g_{max}$*, then go to Step 10. Otherwise, set* $t := t + 1$*, and go to Step 3.*
10. ***Final Intensification.*** *Apply Procedure 3 to obtain* x^{Core}*. Update* DS *by* x^{Core} *if a better solution is found, and terminate.*

4 Numerical Experiments

Algorithm 4 was programmed in MATLAB and applied 18 instances of the MDS problem created from the three graphs G1 - G3, see Table 1. To create the MDS instances, we first generate three graphs by randomly (using uniform distribution) placing n number of nodes in an $M \times M$ area. A minimum and maximum range R is specified for each graph with an increment step of ten to give graphs with different densities as shown in Tables 3 - 8. From these three graphs, 18 problem instances are obtained. For each problem instance, the HGA-MDS MATLAB code was run 20 times with different initial populations.

Table 1. Test Problems

test graphs	No. of Nodes	Range	Distance
G1	80	400×400	60-120
G2	200	1000×1000	100-160
G3	350	2500×2500	200-230

4.1 Parameters Analysis

Before discussing the results of the HGA-MDS, we explain the setting of the HGA-MDS parameters. In Table 2, we summarize all parameters used in HGA-MDS with their assigned values. These chosen values are based on the common setting in the literature or based on our numerical experiments. HGA-MDS parameters are categorized into four groups:

– Initial Parameters: M is the population size.
– GA operator Parameters: p_c and p_m are Crossover probability and Mutation probability, respectively.
– Intensification Parameters: n_l is the number of iterations applied in *LocalSearch*, n_{DS} is the maximum number of the best dominating sets used to update DS, and n_{Core} is the pre-specified number of the n_{DS} best dominating sets used to compute x^{Core}.
– Termination Parameters: g_{max} is the maximum number of generations.

Table 2. HGA-MDS Parameter setting

Parameter	Definition	Value
M	Population size	40
p_c	Crossover probability	0.8
p_m	Mutation probability	0.01
n_l	Number of iterations in *LocalSearch*	2
n_{DS}	Max number of the best dominating sets used to update DS	10
n_{Core}	The number of the best dominating sets used to compute x^{Core}	3
g_{max}	Max number of generations	100

4.2 Results

The performance of the proposed HGA-MDS was tested on 18 instances of the MDS problem created from the three graphs G1 - G3. The results of the HGA-MDS are reported in Tables 3 - 8. In order to demonstrate the effectiveness of the HGA-MDS method, we compare the proposed HGA-MDS against a standard genetic algorithm (GA), and another kind of HGA-MDS with a second fitness function [13], it's computed based on the penalty term that adds the number of uncovered nodes to the fitness function. Whenever two methods (say A and B) are compared in terms of the average numbers (Avg.) and the standard deviation (Std.) of obtained solutions found on a problem instance, we use the t-test to check for statistical significance. The level of significance used in the tests is 0.05. The results of the significance test found on an independent column in all the result Tables (see Tables 3 - 8).

4.3 Performance Comparison of HGA-MDS and GA

The results of this comparison are reported in Tables 3, 4, and 5. All methods have the same number of runs for each graph, which is 20. Among the two methods, HGA-MDS could obtain the best minimum dominating sets for all instances of the MDS problem. All these improvements were obtained for all graphs, and according to the significance test, HGA-MDS demonstrate statistically verified improved solution qualities across the 20 runs for all instances (see t-test columns and refer to Tables 3, 4, and 5). The p values for all compared results in Tables 3, 4, and 5 are less than 0.0001. By conventional criteria, this difference is considered to be extremely statistically significant.

Table 3. Results of HGA-MDS and GA on G1 (No. of nodes = 80, Area = 400×400)

Range	GA			HGA-MDS			t-test of $\gamma(G1)$		
	Best	Avg.	Std.	Best	Avg.	Std.	t-value	Significant	Method
60	17	19.65	1.6630	15	15.75	0.4442	10.1326		HGA-MDS
70	14	16.95	1.2343	12	13.30	0.7326	11.3724		HGA-MDS
80	12	14.65	1.3484	10	11.65	1.0894	7.7396		HGA-MDS
90	10	11.10	0.8522	8	8.05	0.2236	15.4816		HGA-MDS
100	9	10.05	0.6863	7	7.90	0.3077	12.7840		HGA-MDS
110	7	8.00	0.9176	6	6.00	0	9.7475		HGA-MDS
120	6	8.05	0.9445	5	5.55	0.5104	10.4140		HGA-MDS

Table 4. Results of HGA-MDS and GA on G2 (No. of nodes = 200, Area = 1000×1000)

Range	GA			HGA-MDS			t-test of $\gamma(G2)$		
	Best	Avg.	Std.	Best	Avg.	Std.	t-value	Significant	Method
100	58	64.90	3.3544	38	41.25	2.4682	25.3964		HGA-MDS
110	53	58.15	2.7198	33	36.80	1.5423	30.5374		HGA-MDS
120	46	50.90	3.8374	26	28.55	1.5381	24.1771		HGA-MDS
130	39	48.85	3.8970	25	27.05	1.3168	23.7009		HGA-MDS
140	36	42.60	4.5583	22	24.30	1.2607	17.3044		HGA-MDS
150	30	37.90	4.1662	20	21.40	0.9947	17.2274		HGA-MDS
160	29	33.90	2.4899	19	20.50	1.0513	22.1725		HGA-MDS

Table 5. Results of HGA-MDS and GA on G3 (No. of nodes = 350, Area = 2500×2500)

Range	GA			HGA-MDS			t-test of $\gamma(G3)$		
	Best	Avg.	Std.	Best	Avg.	Std.	t-value	Significant	Method
200	113	121.95	4.6052	64	80.66	15.1153	11.6861		HGA-MDS
210	109	117.70	5.3024	59	73.04	4.2426	29.4112		HGA-MDS
220	102	108.85	3.4682	51	57.00	3.8661	44.6459		HGA-MDS
230	93	102.00	4.9417	49	54.95	4.0971	32.7787		HGA-MDS

4.4 Performance Comparison of HGA-MDS and HGA-MDS (With f_p)

The performance of the proposed HGA-MDS on the MDS problem is compared against the HGA-MDS With fitness function is computed based on the penalty term as shown in Equation (2)

$$f_p = \sum_{i=1}^{n} x_i + \mu \cdot \mathit{Uncovered}(x), \tag{2}$$

where μ is the penalty parameter, and the function $\mathit{Uncovered}(x)$ gives the number of nodes in the graph which are not directly linked to any nodes of x. The first term in Equation (2) gives the size of the dominating set, while the second

is the penalty term that adds the number of uncovered nodes to the fitness function. The penalty parameter μ is set to $|V| + 620$. The experiment results comparing HGA-MDS vs. HGA-MDS (With f_p) are reported in Tables 6, 7, and 8. The results shown in these tables clarify the efficiency of the proposed fitness function *fit* given in Equation (1). The p values for all compared results in Tables 3, 4, and 5 are less than 0.0062. By conventional criteria, this difference is considered to be very statistically significant. Moreover, the results in Table 9 show that this fitness function can lead GA to find the solution faster.

Table 6. Results of HGA-MDS on G1 (No. of nodes = 80, Area = 400×400) using two fitness functions

Range	HGA-MDS (With f_p)			HGA-MDS			t-test of $\gamma(G1)$	
	Best	Avg.	Std.	Best	Avg.	Std.	t-value	Significant Method
60	16	24.30	5.5922	15	15.75	0.4442	6.8160	HGA-MDS
70	13	25.35	6.2683	12	13.30	0.7326	8.5390	HGA-MDS
80	11	18.25	6.0600	10	11.65	1.0894	4.7938	HGA-MDS
90	9	18.60	7.2649	8	8.05	0.2236	6.4913	HGA-MDS
100	8	14.85	6.2767	7	7.90	0.3077	4.9459	HGA-MDS
110	7	14.40	7.2358	6	6.00	0	5.1917	HGA-MDS
120	6	14.10	7.8866	5	5.55	0.5104	4.8382	HGA-MDS

Table 7. Results of HGA-MDS on G2 (No. of nodes = 200, Area = 1000×1000) using two fitness functions

Range	HGA-MDS (With f_p)			HGA-MDS			t-test of $\gamma(G2)$	
	Best	Avg.	Std.	Best	Avg.	Std.	t-value	Significant Method
100	50	71.10	14.9240	38	41.25	2.4682	8.8250	HGA-MDS
110	36	60.30	16.6008	33	36.80	1.5423	6.3036	HGA-MDS
120	31	58.25	20.0758	26	28.55	1.5381	6.5967	HGA-MDS
130	27	48.40	20.0850	25	27.05	1.3168	4.7436	HGA-MDS
140	26	52.35	22.3848	22	24.30	1.2607	5.5951	HGA-MDS
150	24	36.45	13.4300	20	21.40	0.9947	4.9979	HGA-MDS
160	21	40.65	21.0869	19	20.50	1.0513	4.2681	HGA-MDS

Table 8. Results of HGA-MDS on G3 (No. of nodes = 350, Area = 2500×2500) using two fitness functions

Range	HGA-MDS (With f_p)			HGA-MDS			t-test of $\gamma(G3)$	
	Best	Avg.	Std.	Best	Avg.	Std.	t-value	Significant Method
200	69	100.20	25.9870	64	80.66	15.1153	2.9067	HGA-MDS
210	63	95.50	32.4369	59	73.04	4.2426	3.0704	HGA-MDS
220	60	74.95	25.0903	51	57.00	3.8661	3.1621	HGA-MDS
230	53	72.95	24.9999	49	54.95	4.0971	3.1776	HGA-MDS

Table 9. The Cost Comparison of HGA-MDS and HGA-MDS with f_p for Graphs G1-G3

Test Graph	Range	HGA-MDS with f_p		HGA-MDS	
		Avg.	Std.	Avg.	Std.
G1	60	15392.85	436.6762	14405.95	140.8099
	70	15473.70	511.5600	14163.65	196.2789
	80	14915.80	484.4066	13635.10	161.4164
	90	14935.65	578.0730	14012.90	110.4731
	100	14630.70	486.5871	13981.85	118.8096
	110	14609.60	551.8655	13880.20	110.9702
	120	14574.55	622.4485	13827.25	105.1209
G2	100	28841.65	2960.732	19144.70	1104.359
	110	26288.55	4107.328	19607.20	751.7671
	120	25668.25	5198.135	19040.30	637.5162
	130	24060.35	4463.898	18720.40	1000.192
	140	25150.95	4449.000	18513.55	565.3216
	150	20981.25	3997.115	18310.55	403.8004
	160	22354.10	4762.851	17931.35	772.7919
G3	200	35444.00	21865.33	22890.24	4063.943
	210	35809.75	22529.19	23280.80	2648.977
	220	26653.10	17584.30	24904.40	2912.662
	230	26634.95	17327.92	24627.75	2189.367

5 Conclusions

The minimum dominating set problem in graph theory has been studied in this paper. A hybrid GA-based method, called hybrid genetic algorithm for minimum dominating set (HGA-MDS), has been proposed to solve the considered problem. New fitness function and intensification elements have been inlaid in HGA-MDS to achieve better performance and to fit the problem. Numerical experiments on 18 graphs have been presented to show the efficiency of HGA-MDS. Comparisons with other methods have revealed that HGA-MDS is promising and it is less expensive.

References

1. Baker, J.E.: Adaptive selection methods for genetic algorithms. In: Grefenstette, J.J. (ed.) Proceedings of the First International Conference on Genetic Algorithms, pp. 101–111. Lawrence Erlbaum Associates, Hillsdale (1985)
2. Burke, E.K., Kendall, G.: Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques. Springer, Berlin (2005)
3. Carey, M.R., Johnson, D.S.: Computers and Intractability: A guide to the theory of NP-Completeness. Freeman, New York (1979)
4. Cooper, C., Klasing, R., Zito, M.: Lower bounds and algorithms for dominating sets in web graphs. Internet Math. 2, 275–300 (2005)

5. Engelbrecht, A.P.: Computational Intelligence: An Introduction. John Wiley & Sons, Chichester (2003)
6. Fomin, F.V., Thilikos, D.M.: Dominating Sets in Planar Graphs: Branch-Width and Exponential Speed-Up. SIAM J. Computing 36, 281–309 (2006)
7. Goldberg, D.E.: Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley, Reading (1989)
8. Grandoni, F.: A note on the complexity of minimum dominating set. J. Discrete Algorithms 4, 209–214 (2006)
9. Haynes, T.W., Hedetniemi, S.T., Slater, P.J.: Domination in graphs. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, New York (1998)
10. Haynes, T.W., Hedetniemi, S.T., Slater, P.J.: Fundamentals of domination in graphs. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, New York (1998)
11. Herrera, F., Lozano, M., Verdegay, J.L.: Tackling real-coded genetic algorithms: Operators and tools for behavioural analysis. Artificial Intelligence Review 12, 265–319 (1998)
12. Ho, C.K., Ewe, H.T.: A hybrid ant colony optimization approach (hACO) for constructing load-balanced clusters. In: IEEE Congress on Evolutionary Computation, pp. 2010–2017 (2005)
13. Ho, C.K., Singh, Y.P., Ewe, H.T.: An enhanced ant colony optimization metaheuristic for the minimum dominating set problem. Applyed Artificial Intelligence 20, 881–903 (2006)
14. Holland, J.: Adaptation in Natural and Artifical Systems. University of Michigan Press, Ann Arbor (1975)
15. Konar, A.: Computational Intelligence: Principles, Techniques and Applications. Springer, Berlin (2005)
16. Korobitsyn, D.V.: On the complexity of determining the domination number in monogenic classes of graphs. Diskret. Mat. 2, 90–96 (1990); in Russian, translation in Discrete Mathematics and Applications 2, 191–199 (1992)
17. Lozin, V., Milanič, M.: Domination in Graphs of Low Degree. Rutcor Research Report (RRR) New Jersey 27 (2006)
18. Müller, H., Brandstädt, A.: NP-completeness of STEINER TREE and DOMINATING SET for chordal bipartite graphs. Theoretical Computer Science 53, 257–265 (1987)
19. Samuel, H., Zhuang, W.: DTN Based Dominating Set Routing for MANET in Heterogeneous Wireless Networking 14, 154–164 (2009), Springer
20. Tettamanzi, A., Tomassini, M., Janben, J.: Soft computing: integrating evolutionary, neural, and fuzzy systems. Springer, Berlin (2001)

Proactive Identification and Prevention of Unexpected Future Rule Conflicts in Attribute Based Access Control*

Daren Zha[1], Jiwu Jing[1], Peng Liu[2], Jingqiang Lin[1], and Xiaoqi Jia[1,2]

[1] SKLOIS,Graduate University of CAS, Yuquan Road, 19A, Beijing 100049, China
[2] College of IST, The Pennsylvania State University, University Park, PA 16802, USA
zdr@is.ac.cn, jing@is.ac.cn,
pliu@ist.psu.edu, linjq@is.ac.cn, xqjia@is.ac.cn

Abstract. Attribute based access control (ABAC) provides an intuitive way for security administrators to express conditions (associated with status of objects) in access control policies; however, during the design and development of an ABAC system, new problems concerning the consistency and security of the ABAC system may emerge. In this paper, we report on two specific ABAC problems denoted as the "future rule conflicts" problem and the "object overlapping" problem, which we have recently identified in developing the ABAC system for a large research laboratory. We use real world examples to illustrate the negative impact of these two problems and present two novel algorithms for the identification and prevention of these problems. We give the correctness proof for both algorithm and apply these algorithms to the attribute based laboratory control (ABLC) system and the results are also reported.

Keywords: ABAC, future rule conflicts, object overlapping.

1 Introduction

Attribute based access control (ABAC) in many situations is a good complement to role based access control (RBAC) which has been a main research and development area in access control for several years (e.g., [16], [6], [3], [12], [15], [17]). ABAC provides an intuitive way for security administrators to express conditions (associated with status of objects) in access control policies. In addition, attributes (of subjects and users) can be used by administrators to identify the needs to create new roles, "split" or "merge" existing roles, or remove roles that are no longer useful.

We have recently applied ABAC in developing the ABLC system for a large research laboratory consisting of 200 staff and graduate students. During this practice, we conclude the basic requirements of ABAC, and find two new problems (within ABAC system design and implementation): the "future rule conflicts" problem and the "object overlapping" problem. These two problems can

* This work is supported by 863 Foundation No.2006AA01Z454, and NSF No.70890084/G021102.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 468–481, 2010.

harm the consistency and the security of the ABAC systems we are concerned with. Identification and prevention of these problems can evidently improve the safety and usability of ABAC systems. In this paper we set out to show the algorithms which can be used to solve the two problems.

The primary contributions of our work are:

- We are the first to generalize the basic requirements of ABAC.
- Our work is the first to discover and give the identification and prevention algorithm for the problem named "future rule conflicts" in ABAC. We also prove the correctness of the algorithms.
- We report new findings about "Object Overlapping" problem in ABAC. We also present our algorithm for "object overlapping" and prove the correctness.

1.Basic requirements of ABAC. ABAC has a strong ability to express different attributes and attribute-based predicates for both subjects and objects, so ABAC is a valuable complement to existing access control mechanisms. However, ABAC also has its disadvantages, such as a large number of domain values for some attributes and difficulty in managing a large set of attributes. During the development of the ABLC system, we have had a good number of observations on what a good ABAC system should look like.

2.Proactive Identification and prevention of future rule conflicts. Due to the large number of attributes, consistency is one of the basic requirements in ABAC. There are various methods to check the consistency of an access control system at a specific point of time, however, we found that such methods cannot identify and prevent future rule conflicts in ABAC. We show the problem called unexpected future rule conflicts in ABAC in Section 3.1, analyze the problem and give the solving algorithm in Section 4.

3.Identification and prevention of object overlapping. For one object in ABAC, there may be more than one modeling method for it. Rule maker can use any of these modeling methods for the object, however, if rule makers use more than one method for the same access control system, object overlapping may occur. We first show why the object overlapping problem could exist, then we discuss two different solving mechanisms, one in the design phase, the other in the implementation phase.

The rest of the paper is organized as follows. We generalize the basic requirements of ABAC in Section 2. We discover the problems called " future rule conflicts" and "object overlapping" in Section 3. We present our approach of identification and prevention the both problems and the correctness proof in Section 4, 5 and 6. We compared our work with related work in Section 7.

2 Basic Requirements of ABAC Rule Management

In this section, we analyze the basic requirements of ABAC. These requirements serve as guiding principles to develop the access control system for our laboratory. We start by finding the needs of the system, then set up an abstract model, present the basic definitions and theorem, and outline the requirements.

2.1 Motivation

Our laboratory is in critical needs of an access control system due to the diversity of the user's background, the scattered allocation of workrooms and the different security levels of its equipments. In order to make full use of the resources and prevent an information leakage, we need to build an appropriate access control system.

We first adopted RBAC in building the access control system. However, when we tried to make rules for the storing server, we discovered the limitations of the RBAC in modeling the attribute for the accessed object, whereas the status of the server is an indispensable element of the access rules. The reason is that the the administrator should not adjust the configuration to interrupt the services when the server is in a normal status. The necessity of adjustment only arises when the server is in an unknown or break down status. Specifically, when the server is in an unknown or break down status, RBAC can not model the server with a specific status for the server as an object, which will lead to the unsolved condition, causing problems for both administrators and users. For administrators, the task of rule making will be extremely difficult without the status of the server. For users, they are likely to be confused by objects without attributes. To avoid the above-mentioned problems and to acquire more usability, we chose ABAC in the development of our access control system, which is named as attribute based laboratory control system.

2.2 Model of ABAC

As shown in Fig.1, we construct a formal model in terms of sets and relations to clarify the notions of ABAC.

For each rule $\mathbb{r}$ in ABAC, it can be defined as a five-tuple $\{\mathcal{P}/\mathcal{D}, \mathcal{S}, \mathcal{O}, \mathcal{A}, \mathcal{C}\}$. $\mathcal{P}/\mathcal{D}$ represents whether the rule permits($\mathcal{P}$) or denies($\mathcal{D}$) the actions, $\mathcal{S}$ is the set of subject's attributes, $\mathcal{O}$ is the set of objects' attributes, $\mathcal{A}$ is the set of actions in the rule, and $\mathcal{C}$ is the set of constraints in the rule.

We can define each rule $\mathbb{r}$ in the following format: $\mathbb{r} = \{\ \mathcal{P}/\mathcal{D}, \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n\}, \{\mathcal{O}_1, \mathcal{O}_2, \ldots \mathcal{O}_n\}, \{\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_n\}, \{\mathcal{C}_1, \mathcal{C}_2, \ldots \mathcal{C}_n\}\ \}$

The sample rule shown in Fig.3 means that only the power administrator can adjust the power switcher in his working room when the status of power is normal. All the predicates like "native" and "administrator" can get an attribute either from the subject or from the object.

2.3 Basic Requirements of ABAC

During the rule making process, we conclude that there are six basic requirements for ABAC design and two requirements for its development, as the Fig.2 shows.

Completeness. The requirement of completeness should be satisfied both in terms of rules and attributes. If the attributes are incomplete, the rules will be incomprehensive leading to unpredictable errors in the enforcement of access control.

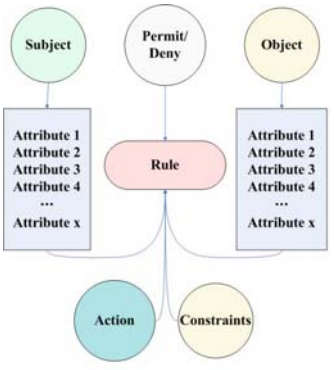


Fig. 1. The model of ABAC

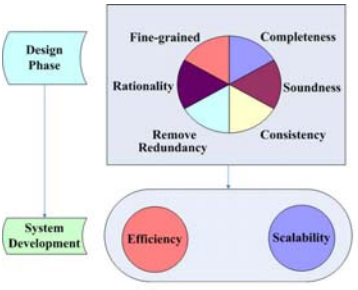


Fig. 2. Basic Requirements of ABAC

$$r_S = \{P, \{native, administrator, administrativezone.eq(power), place.eq(ps.place)\}, \{status.eq(normal)\}, \{read, expand, write, delete\}, \{8:30 < time < 12:00 || 13:00 < time < 17:30\}\}$$

Fig. 3. Sample Rule

Soundness. Soundness means that every rule must be correct in regards to the current situation. However, this is arguably an unattainable goal (unless we invent a technique that can predict every possible change in the future). In actual practice, we may obtain the best rules by constantly testing and bug-fixing.

Consistency. In ABAC, this requirement should be strictly satisfied because the conflicts in the rules may confuse the users and the enforcement engine of the access control system. This sort of problems will be expounded on in Section 3.1. The identification and prevention of these problems will be provided in Section 4.

Remove redundancy. In ABAC, there are always hundreds of attributes and rules, whereas too many redundant attributes or rules may cause difficulty for comprehension as well as system development. Sorting out the rules could be a viable solution to this problem, moreover, the administrator can sort out the rules according to his/her own opinions.

Rationality. A rational ABAC system is one with suitable modeled objects, however, not all methods available during the rule making process are suitable for a specific environment. For example, for a web server, whether a user can read or write on a folder is more important than the storage of the disk occupied by users, thus to model a web server on the basis of folders with rights is more rational than modeling it on the basis of sectors or disks.

Fine-grained. Possessing fine-grained access control is one goal for most systems, including the system using ABAC. There are some challenges for developing

a fine-grained access control system, such as the way to model the object into pieces, to sort the rules into the rule set, and whether or not some optional attributes should be included.

We will turn to the two basic requirements in the ABAC system development, namely, ***efficiency*** and ***scalability***. Efficiency should be taken into account in the process of system development so as to ensure the efficient enforcement of access control. Compared with the RBAC system, the ABAC system holds more attributes, which entail a larger number of rules. Under such circumstance, efficiency can be achieved through the rational organization of all the rules and the utilization of a suitable algorithm. Good scalability is necessary for the upgrading or the adjustment of the ABAC system, which are unavoidable if the access control system serves a long time.

3 Problem Statement and Design Goals

After putting forward the requirements for ABAC, an important step in constructing our ABLC system will be to scope the problems we need to solve and reveal the challenges inherent in the problems. In this section, We will describe the problems likely to cause unexpected rule conflicts and object overlapping.

3.1 Problem 1: Unexpected Future Rule Conflicts

During the rule-making process, although rules seemed to be sound at the time of rule-making, hidden conflicts were quite likely to appear in future. We use the following example to further illustrate this problem. Firstly, we make rule $\mathtt{r}_1$ and $\mathtt{r}_2$ as follows:

$$
\begin{aligned}
\mathtt{r}_1 = &\{P, \{native, administrator, administrativezone.eq(applicationserver),\\
&place.eq(402)\}, \{status.eq(normal), WorkingProject.eq(wholelab)\},\\
&\{read, expand, write, delete\}, \{8:30 < time < 12:00 || 13:00 < time < 17:30\}\}\\
\mathtt{r}_2 = &\{D, \{native, age.leq(20)\}, \{status.eq(normal), WorkingProject.eq(wholelab)\},\\
&\{read, expand, write, delete\}, \{8:30 < time < 12:00 || 13:00 < time < 17:30\}\}
\end{aligned}
$$

Fig. 4. Conflicts Rules for application server

The $\mathtt{r}_1$ means the person who is the administrator in charge of application server and can adjust the configurations of application server in normal status. Also, with the same notations, we have another rule $\mathtt{r}_2$ for the application server as shown in Fig.4. In the beginning, the two rules run well, however, when an 18-year old Ph.D student becomes the administrator of the application on some day, $\mathtt{r}_1$ permits the his access to application server while $\mathtt{r}_2$ denies. The two rules were right are now in conflict. We did some research on this event, and found that the conflicts can be attributed to the following factors. Firstly, one attribute value of one subject can be mapped to a group of subjects, that is to say, more than one subject have the same attribute value. In fact, in ABAC, the essence

of rule definition by attributes is picking out all the corresponding subjects or objects which have the same attributes. Secondly, different attributes may be used to apply the same action of access control to the same object by different rule makers. The essence of this method is that access control is concerned with more than one attributes in a specific scenario. Finally, in a specific scenario, using different methods to organize attributes for the subject may finally result in the future conflicts.

From the above three factors, we can see how the unexpected rule conflicts take place in Fig.5. A formal definition is given as follows:

Definition 1 (**Future Rule Conflicts):** Two rules $\mathbb{r}_1$ and $\mathbb{r}_2$ may cause *future rule conflicts* if the following four conditions are all satisfied:

(a)One rule holds $\mathcal{P}$ and the other holds $\mathcal{D}$.

(b)$\mathbb{r}_1$ and $\mathbb{r}_2$ have the same action in $\mathcal{A}$.

(c)$\mathbb{r}_1$ and $\mathbb{r}_2$ are used for the access to the same object with the same object attributes set $\mathcal{O}$ and with the same constraints set $\mathcal{C}$.

(d)Intersection which is produced by $\mathcal{S}$ for $\mathbb{r}_1$ and $\mathcal{S}$ for $\mathbb{r}_2$ is not empty and the values in the intersection can be suitable for one subject. □

Here we should clarify what is "current" and what is "future" in the definition of *future Rule Conflicts*. In condition d, if the specific subject with these attributes is a current user in the system, we define the conflicts as "current" ones. If the subject does not exist currently, but is likely to appear in the future, we define the conflict as "future" rule conflicts. From these facts, we draw the conclusion that "current" conflicts can be evolved into "future" conflicts without alerting our ABAC system and solving algorithm. The solving algorithm will be discussed in Section 6.

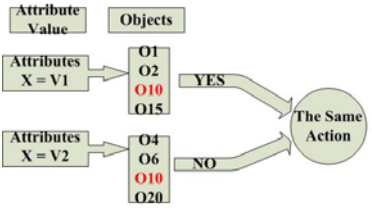


Fig. 5. Conflict event

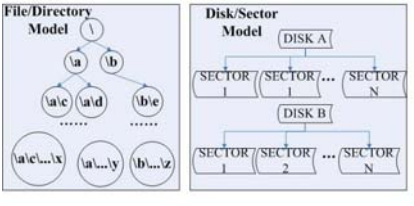


Fig. 6. Different modeling method for storing server

3.2 Problem 2: Object Overlapping

In this subsection, we will discuss another question pertaining to the requirement of consistency. Object modeling is a critical component in the ABAC system design. Sometimes there are more than one modeling method for a single object, and the different modeling methods may have their own advantages. However,

if the objects are modeled by more than one method, the system may produce the fault of object overlapping. This will lead to some problems.

As shown in Fig.6, we have two modeling methods to organize the storing server in ABLC system. One method depends on the directory and files. It is convenient to exert access control over files and folders of which the ownership is fixed. Another method regards the disks and sectors. It will be especially convenient for the storing server's access control to calculate the total bytes occupied by the user.

Since advantages of both methods could not be fully achieved when they were used separately, we tried to apply both methods to our control system. However, the system may have problems in enforcement owing to the occurring object overlapping. When one access request concerning the overlapping object comes into the access control system, the system may find that there are more than one rule to be taken for the request if the following two conditions are both satisfied. Firstly, these rules should contain the same action, object attributes set and constraints set. Secondly, the attributes of subjects provided in the request should be satisfied for a multiple rules.

From the above facts, we summarize how object overlapping happens in Fig.6.

Definition 2 (Object Overlapping): Two rules $\mathbb{r}_1$ and $\mathbb{r}_2$ may have *object Overlapping* if the following four conditions are all satisfied:

(a)$\mathbb{r}_1$ and $\mathbb{r}_2$ are used for the access to the same object with the same object attributes set $\mathcal{O}$.
(b)$\mathbb{r}_1$ and $\mathbb{r}_2$ should be enforced under the same constraints set $\mathcal{C}$.
(c)$\mathbb{r}_1$ and $\mathbb{r}_2$ are used for at least one same action in $\mathcal{A}$.
(d)$\mathcal{S}$ in one rule is contained by the $\mathcal{S}$ in the other rule. □

To solve the object overlapping, we will discuss in Section 6 the algorithm which is based on definition 2.

4 Solving Future Rule Conflicts

To identify and prevent potential rule conflicts in rule designing, we first divided the rule set into single rules for pre-process. We then listed all the attributes and actions in these rules and analysis. Once we determine whether or not future conflicts may happen, we incorporated the results and rule fixing to promote the use of rule set.

Firstly, we can see the pre-process algorithm in Fig.7.

4.1 Solution From Attributes Comparison

To avoid future rule conflicts, we found during the design phase the identification is more critical and the special attributes set given by identification can be used directly for prevention. After the identification, the prevention can be done by the administrator according to the context much more easily. Next, we can consider the example in the above section, and refer to the two rules which will be in conflict in future in Fig.5 again.

```
(1)class Rule {
(2)    public Boolean decision;
(3)    public int action;
(4)    public int constraints;
(5)    public object obj;
(6)    public object sbj;
(7)}
<Pre-process>
(8) Initialize RuleArray[NumOfRule];
(9) IndexOfRule = 1;
(10)While(RuleSet !=NULL)
(11)    {
(12)     RuleArray[IndexOfRule] = FirstRule in RuleSet;
(13)     IndexOfRule ++;
(14)     RuleSet = RuleSet - FirstRule;
(15)    }
(16)Output RuleArray;
```

Fig. 7. Pre-process Algorithm

Considering the above scenario, we try to develop the algorithm for solving future conflicts. In the first step, we should make sure that the compared rules have the same object attributes and constraints. In sample rule $\mathbb{r}_1$ and $\mathbb{r}_2$, we can find that two rules have the same object attributes set {status.eq(normal), WorkingProject.eq(whole lab)}, and the same constraints set {8:30<time<12:00 || 13:00<time<17:30}. Also we should compare the actions of all the rules. If two rules hold opposite decisions for at least the same action to the same object, we can speculate that there might be some future conflicts. In the sample rules, we can find that $\mathbb{r}_1$ permits action set {read, expand,write, delete}, while $\mathbb{r}_2$ denies the same action set. They have different decisions for the same action to the same object, so we can move on to the second step.

Secondly, we start identification from the attributes of subject in pairs which we acquired in the first step. For each pair we get all the attributes for the subject in the rule, because subject only stands for person in our control system, we can find the attribute set for each rule in the pairs we got from the first step. In $\mathbb{r}_1$, we can get subject attributes set {native, administrator, administrative zone.eq(application server), place.eq(402)}. In $\mathbb{r}_2$, we get {native, age.leq(20)} in the same way.

Thirdly, we delete the same attribute from the second step and compose the attribute set. In the example, we compose both sets and get the set {native, administrator, administrative zone.eq(application server), place.eq(402), age.leq(20)}. The attribute "native" appears only once because this is the same for both $\mathbb{r}_1$ and $\mathbb{r}_2$.

In the last step, we compose the meaningful domain from the two attributes set we got from the third step. If they cannot transform into any reasonable subject for accessing the object in the rules, there can't be any future rule conflicts, however, if the concreted value can exist as a meaningful subject (which may be not in the control system now), we can conclude that there will be future conflicts from the compared rules. In the example, we can see that the attributes set {native, administrator, administrative zone.eq(application server), place.eq(402), age.leq(20)}. If we compose the reasonable values from these attributes, then we can find the value for the less-than-20-year-old administrator

```
<ProcessStepOne&ProcessStepTwo>
 (1)IndexOfSelected = 1;
 (2)TotalSubsetNum = (NumOfRule)(NumOfRule-1)/2;
 (3)Initialize AttributeSetPair[TotalSubsetNum][2];
 (4)for (OutCycleIndex= NumOfRule; OutCycleIndex > 2;OutCycleIndex--)
 (5){
 (6)for (InCycleIndex= OutCycleIndex;InCycleIndex> 1;InCycleIndex--)
 (7)    {
 (8)RuleOne = RuleArray[OutCycleIndex];
 (9)RuleTwo=RuleArray[InCycleIndex];
 (10)  if(!IntersectionAction(RuleOne,RuleTwo))
 (11)&&(GetActionObject(RuleOne) == GetActionObject(RuleTwo))
 (12)&&(GetActionConstraints(RuleOne)==GetActionConstraints(RuleTwo))
 (13)&&(GetDecision(RuleOne) != GetDecision(RuleTwo))
 (14)       {
 (15)     AttributeSetPair[IndexOfSelected][1]=GetAttribute(RuleOne);
 (16)     AttributeSetPair[IndexOfSelected][2]=GetAttribute(RuleTwo);
 (17)     IndexOfSelected ++;
 (18)       }
 (19)     }
 (20)}
<ProcessStepThree>
 (21)Initialize ProcessedAttribute[IndexOfSelected];
 (22)for(IndexOfProcessed = 1;IndexOfProcessed <= IndexOfSelected;
 (23)IndexOfProcessed ++ )
 (24){
 (25)ProcessedAttribute[IndexOfProcessed] =
 (26)DeleteTheSameAttribute(AttributeSetPair[IndexOfProcessed][1],
 (27)AttributeSetPair[IndexOfProcessed][2]);
 (28)}
<ProcessStepFour>
 (29)Initialize ConflictsRuleSet[IndexOfSelected];
 (30)for (Index=1;Index<=IndexOfProcessed; Index ++) {
 (31)if (ProcessedAttribute[index] != NULL)
 (32)  {
 (33)  if(!ConcreteDomain(ProcessedAttribute[index]))
 (34)  ConflictsRuleSet[Index] = ConcreteDomain
 (35)  (ProcessedAttribute[index]);
 (36)  }
 (37)}
 (38)Output ConflictsRuleSet;
```

Fig. 8. Solution Algorithm For Rule Conflicts

who works in Room 402 can be occupied by the two sets. We can draw the conclusion that if one administrator younger than 20 years old comes into the control system, the two rules will have future conflicts. Also the identification gives out the special attribute for our initial rule set. After discussion, we finally modify the attribute "age.leq(20)" into "age.leq(12)" in the *INITIAL* rule because maybe it's unfair to the young administrator. The whole algorithm is shown for the process in Fig.8.

4.2 Result of Algorithm for Future Rule Conflicts

We have used the algorithm to find some future rule conflicts, and we show them in Table 1. The first one is shown in the example, and the second conflicts start from an initial rule which says that a person with medium technique cannot adjust the power switcher. Conflicts happen when the Ph.D student becomes a teacher in the laboratory while still holding the job as the administrator. After the identification, we resolved all the identified conflicts by adjusting all the attributes listed in the rules.

Table 1. Future rule conflicts found in INITIAL rule set

Num.	Object for Conflicts	Reason
1	application server	one 18 year-old administrator exists in system
2	power switcher	a p.h.d student becomes a teacher

5 Complexity Analysis and Correctness Proof for Finding Future Rule Conflicts

Now we look into the complexity analysis of the algorithm in Fig.8. Assuming N for a total number of rule, in circle of Step One and Step Two, the time complexity will be $N \times (N-1)$. In Step three and Step four, the complexity will both be $O(N)$. In total, the complexity for the algorithm is $O(N \times (N-1)) + O(N) + O(N) = O(N^2)$.

We also analyze the dimension of completeness. Future rule conflicts means two rules in future for the same subject have the same $\mathcal{O}$, $\mathcal{A}$ and $\mathcal{C}$, but $\mathcal{P}$s are opposite. In the control system rule set, there may be hundreds of rules, so we should start by searching the same and opposite factors such as $\mathcal{O}$, $\mathcal{A}$, $\mathcal{C}$ and $\mathcal{P}$ in the whole rule set. That is step one in our solution, through this step we can pick up all rules likely to cause future rule conflicts. The next task is to pick up all the possible situations in which future rule conflicts will take place. That is to say, we should search for the key attributes set $\mathcal{S}$, which will lead to the conflict in the future. So we deal with the rule pairs in the first step, trying to find their attributes set and compose the attributes set. This is done by step two and three in our algorithm. At last, the situation for future rule conflicts is equal to the meaningful subject that has the same attributes set with concreted set. We start from the rule set in the control system and deal with all possible rule pairs. We can see that the algorithm is complete.

Let us prove the correctness of the algorithm: Firstly, the number of rules in the system is finite, so our algorithm can finish the task within finite time. Secondly, if the concreted attributes can be held by one subject, the selected rules will be in conflict with each other in the future. So the requirements of the soundness of algorithm can be satisfied. Thirdly, the completeness have been proven in the above paragraph. Accordingly, we may conclude that the algorithm is correct.

It should also be noticed that there are only attributes from one single object in the sample rule. Sometimes one rule may relate to more than one object. For example, in our laboratory, if the network device is in an abnormal status, the administrator may have to turn off the power switcher. In this scenario, the access to the power switcher depends on the status of the network device. The rule for the access to power switcher contains the attributes from two objects, namely the power switcher and network device.

6 Solving Object Overlapping

The problem of object overlapping is discussed in Section 3.2. Here we also show an example of the storing server.

```
<Object Overlapping Identification>
 (1)Initialize ObjOverlappedRulesPair[TotalSubsetNum][2]
 (2)for (OutCycleIndex= NumOfRule; OutCycleIndex > 2;OutCycleIndex--)
 (3){Rule tempoutrule = RuleArray[OutCycleIndex]
 (4) for (InCycleIndex= OutCycleIndex-1;InCycleIndex> 1;InCycleIndex--)
 (5) {Rule tempinrule = RuleArray[InCycleIndex];
 (6) if(!IntersectionAction(tempoutrule,tempinrule)&&
 (7)  &&(GetActionObject(tempoutrule) == GetActionObject(tempinrule))
 (8)  &&(GetActionConstraints(tempoutrule)==
 (9)GetActionConstraints(tempinrule)))
 (10)  &&((Belong(tempoutrule.sbj,tempinrule.sbj))||
 (11)    (Belong(tempinrule.sbj,tempoutrule.sbj)))
 (12) ObjOverlappedRulesPair[OutCycleIndex][1] =tempoutrule;
 (13) ObjOverlappedRulesPair[OutCycleIndex][2] =tempinrule;
 (14) }
 (15)}
 (16)Output ObjOverlappedRulesPair;
```

Fig. 9. Object Overlapping Identification

6.1 Identification for Object Overlapping

From our researches, object overlapping is mainly generated during the rule making process. For each resource to be accessed, the modeling methods are decisive for the rule design. The object overlapping originates from the different modeling methods for the same object in the same rule set. If we want to identify the object overlapping, we also need to find the different modeling instances for the same object in the same rule set.

We obtain all the rules from rule set with the pre-process algorithm shown in Fig.7. With all the rules, we begin our identification. According to the model of ABAC, we know that each rule $\mathbb{r}$ can be defined as a five-tuple $\{\mathcal{P}, \mathcal{S}, \mathcal{O}, \mathcal{A}, \mathcal{C}\}$. If $\mathcal{O}$, $\mathcal{A}$ and $\mathcal{C}$ are all the same for two rules $\mathbb{r}_1$ and $\mathbb{r}_2$, and the $\mathcal{S}$ in one rule is contained by the $\mathcal{S}$ in the other rule, then $\mathbb{r}_1$ and $\mathbb{r}_2$ should be enforced at the same time. Otherwise the access control enforcement in control system can't be operated.

Depending on the above facts, we summarize the algorithm for detecting object overlapping in the ABAC system. The algorithm is shown in the following Fig.9.

6.2 Result of Algorithm for Object Overlapping

We also applied the algorithm in 9 to the *INITIAL* set of rules in ABLC. We have used the algorithm to find object overlapping, and we show the results in Table 2. The first row in Table 2 is our example. In the second row, first we used two kinds of modeling methods, one on the basis of different security levels, and

Table 2. Object Overlapping found in INITIAL rule set

Num.	Object for Overlapping	Reason
1	storing server	modeling for both directory and disk amount
2	filing cabinet	modeling for security levels and storage capability
3	exchange server	modeling for email directory and email amount

the other on the basis of storage capabilities. As is shown in Row Three, we also model the email server on the basis of directory as well as the email amount.

After the identification, we resolved all the identified overlapping list in the Table 2.

6.3 Complexity Analysis and Correctness Proof for Identification Object overlapping

The complexity analysis of algorithm shown in Fig.9 is as follows. Assuming N as the total number of rules, in the first circle, because the number of objects is smaller than the number of rules, the complexity of first circle is $O(N^2)$, and the last circle is $O(N)$. The total complexity of the algorithm is $O(N^2) + O(N) = O(N^2)$.

Let us prove the correctness of the algorithm in three steps: Firstly, since the number of rules in the system is finite, identifying can be finished within finite time. Secondly, the comparisons in the identification algorithm are sufficient according to the definition of object overlapping. Thirdly, all the rules can be processed in that the algorithm starts from the whole rule set. According to the above three factors, we draw the conclusion that the algorithm is correct.

6.4 Discussion

We discovered all the problems from the actual system development, so the basic requirements may need some changes to be more refined. We generalized eight basic requirements from observations during our development. The algorithms developed for resolving future rule conflicts and object overlapping are general in that we all start from rule set and come to the conclusion for general data structure. It's independent of the underlying system, as well as the rule specification language.

Through our research, we conclude that there are mainly two solving mechanism to prevent object overlapping. One way is by using only one modeling method during the rule-making process. Each modeling way is available in this way. Another way is that we can use both modeling methods during rule-making, and we can use an extra mechanism in development, which is called "the combined rule" as an atomic operation.

Our system uses all these attributes and rules based on the common database, so we didn't use any method in the algorithms to enhance the efficiency in searching, however, some access control systems may need this method for searching and storing. In such a scenario, the algorithm can be more simply derived from our algorithm.

7 Related Work

There has been much work on access control for several decades. Among these, some researches are relevant to attributes of rule (e.g., [7], [1], [5]), however, these prior researches basically use attributes to gain the fine-grained results based on the traditional access control(e.g., RBAC). Some RBAC extensions (e.g., [4])

based on the core RBAC model are designed to handle the status (attribute) of the access control entities. Our approach differs from these researches in the basic modeling method. We model all the entities in *attributes* instead of *roles*, and we can use a large amount of attributes. The role number in a system should be limited.

The objectives of our work are related to those of rule conflicts, which have been researched for many years. However, the existing rule conflicts researches are mostly conducted under the context of logic programming, database and machine learning. Many researches (e.g., [8],[9]) deal with a set of derivation rules $\{\mathbb{r}_i\}$, if there exists a database $\mathcal{D}$ such that for some fact α, one can derive both α and not (α) from $\mathcal{D}$ and $\{\mathbb{r}_i\}$. Many researches on machine learning also focus on rule conflicts(eg.[14], [13]). In contrast, our research does not seek evidence from the database or the result of machine learning. We only deal with the attribute based rules with the *attribute* values to find the rule conflicts in the *future*.

Our research is related to research on the detection and resolving of policy misconfigurations. The use of graph-based specification formalisms for detecting conflicts in access model (eg.[10],[11]) has been treated for many years. Our work differs from them in mainly two ways. First, our algorithm explored the conflicts depending on the actual attribute based rule set. Second, we didn't use formal methods, such as a graph-based method. Most recently, Lujo Bauer et al. ([2]) also considered rule misconfigurations problem in their proposed work for improving the usability of any access control systems. They apply association rule mining to the *history* of access attempts to predict changes to access control systems. Our techniques are complementary because we focused on predicting the future rule conflicts with only domain values of attributes.

8 Conclusion

Attribute based access control can express the attributes of objects. It is very useful in access control systems and is flexible for many scenarios, such as a laboratory. We demonstrated that in our ABLC system and put forward the basic requirements of ABAC. Specifically, we found the problems of future rule conflicts and object overlapping, which are critical in developing the control system with ABAC. Next we presented the algorithm for solving these problems, and we also applied the algorithm to resolve the future rule conflicts and object overlapping in our ABLC system. Finally we discovered some future conflicts and fixed the rules timely.

References

1. Al-Kahtani, M.A., Sandhu, R.: Induced role hierarchies with attribute-based rbac. In: SACMAT 2003: Proceedings of the eighth ACM symposium on Access control models and technologies, pp. 142–148. ACM, New York (2003)
2. Bauer, L., Garriss, S., Reiter, M.K.: Detecting and resolving policy misconfigurations in access-control systems. In: SACMAT 2008: Proceedings of the 13th ACM symposium on Access control models and technologies, pp. 185–194. ACM, New York (2008)

3. Beznosov, K., Deng, Y.: A framework for implementing role-based access control using corba security service. In: RBAC 1999: Proceedings of the fourth ACM workshop on Role-based access control, pp. 19–30. ACM, New York (1999)
4. Covington, M.J., Long, W., Srinivasan, S., Dev, A.K., Ahamad, M., Abowd, G.D.: Securing context-aware applications using environment roles. In: SACMAT 2001: Proceedings of the sixth ACM symposium on Access control models and technologies, pp. 10–20. ACM, New York (2001)
5. Cruz, I.F., Gjomemo, R., Lin, B., Orsini, M.: A location aware role and attribute based access control system. In: GIS 2008: Proceedings of the 16th ACM SIGSPATIAL international conference on Advances in geographic information systems, pp. 1–2. ACM, New York (2008)
6. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed nist standard for role-based access control. ACM Trans. Inf. Syst. Secur. 4(3), 224–274 (2001)
7. Vipul, G., Omkant, P., Amit, S., Brent, W.: Attribute-based encryption for fine-grained access control of encrypted data. In: CCS 2006: Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98. ACM, New York (2006)
8. Ioannidis, Y.E., Sellis, T.K.: Conflict resolution of rules assigning values to virtual attributes. In: SIGMOD 1989: Proceedings of the 1989 ACM SIGMOD international conference on Management of data, pp. 205–214. ACM, New York (1989)
9. Jagadish, H.V., Mendelzon, A.O., Mumick, I.S.: Managing conflicts between rules (extended abstract). In: PODS 1996: Proceedings of the fifteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, pp. 192–201. ACM, New York (1996)
10. Koch, M., Mancini, L.V., Parisi-Presicce, F.: Conflict detection and resolution in access control policy specifications. In: Nielsen, M., Engberg, U. (eds.) FOSSACS 2002. LNCS, vol. 2303, pp. 223–237. Springer, Heidelberg (2002)
11. Koch, M., Parisi-Presicce, F.: Formal access control analysis in the software development process. In: FMSE 2003: Proceedings of the 2003 ACM workshop on Formal methods in security engineering, pp. 67–76. ACM, New York (2003)
12. Li, N., Mao, Z.: Administration in role-based access control. In: ASIACCS 2007: Proceedings of the 2nd ACM symposium on Information, computer and communications security, pp. 127–138. ACM, New York (2007)
13. Lindgren, T.: Methods for rule conflict resolution. In: Boulicaut, J.-F., Esposito, F., Giannotti, F., Pedreschi, D. (eds.) ECML 2004. LNCS (LNAI), vol. 3201, pp. 262–273. Springer, Heidelberg (2004)
14. Lindgren, T.: On handling conflicts between rules with numerical features. In: SAC 2006: Proceedings of the 2006 ACM symposium on Applied computing, pp. 37–41. ACM, New York (2006)
15. Park, J.S., Sandhu, R., Ahn, G.-J.: Role-based access control on the web. ACM Trans. Inf. Syst. Secur. 4(1), 37–71 (2001)
16. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. IEEE Computer 29(2), 38–47 (1996)
17. Stoller, S.D., Yang, P., Ramakrishnan, C.R., Gofman, M.I.: Efficient policy analysis for administrative role based access control. In: CCS 2007: Proceedings of the 14th ACM conference on Computer and communications security, pp. 445–455. ACM, New York (2007)

Termination of Loop Programs with Polynomial Guards*

Bin Wu[1], Liyong Shen[2,**], Zhongqin Bi[1,3], and Zhenbing Zeng[1]

[1] Shanghai Key Laboratory of Trustworthy Computing,
East China Normal University, Shanghai, 200062, China
[2] School of Mathematical Sciences,
Graduate University of CAS, Beijing, 100049, China
lyshen@gucas.ac.cn
[3] College of Computer and Information Engineering
Shanghai University of Electric Power, Shanghai 200090, P.R. China

Abstract. Termination analysis of loop programs is very important in many applications, especially in those of safety critical software. In this paper, the termination of programs with polynomial guards and linear assignments is simplified to decide solvability of semi-algebraic systems(SAS). If the number of functions are finite or the functions are integer periodic, then the termination of programs is decidable. The discussion is based on simplifying the linear loops by its Jordan form. And then the process to find the nonterminating points for general polynomial guards is proposed. For avoiding floating point computations in the process, a symbolic algorithm is given to compute the Jordan form of a matrix.

1 Introduction

From the very beginnings of formal analysis of software [1] [2], the task of formally verifying the correctness of a program has been decomposed into proving partial correctness and proving termination separately. Termination analysis is one of the building blocks of automated verification. For a generic loop

```
while (conditions) {commands}
```

it is well known that the termination problem is undecidable in all but the most simple cases[3]. In recent years, a lot of efforts on termination analysis have been achieved.

The classical method to to analyze termination is based on the synthesis of ranking function. Several methods have been presented in [4,5,6,7,8,9] on the synthesis ranking functions. For instance, A.R. Bradley et al [7] can discover linear ranking functions for any linear loops over integer variables based on building ranking function templates and checking satisfiability of template instantiations that are Presburger formulas. The method is complete but neither efficient nor terminating on some loops. In [9], Y.H. Chen proposed a method of discovering nonlinear ranking functions by solving the

* This research was supported in part by NSFC(No. 90718041).
** Corresponding author.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 482–496, 2010.

semi-algebraic systems. Besides these, some other methods ([10,11,12,13,14,15,16,17]) are available to analyze the termination of loop programs. For instance, [10] analyzed finite difference trees to prove termination of multipath loops with polynomial guards and assignments. In [15], A. Tiwari proves that the termination of a class of single-path loops with linear guards and assignments is decidable, providing a decision procedure via constructive proofs. M. Braverman[16] generalized the work of A. Tiwari, and showed that termination of a simple of class linear loops over the integer is decidable.

However, now of the previewed work deals with termination proving for loop programs with polynomial guards, and linear assignments. And we presented a decidable situation for the functions in the SASs are integer periodic. The symbolic technique is introduced to avoid floating point errors in computation. The rest of this paper is organized as follows. Section 2 we define some basic notions. In Section 3 onwards, we focus on polynomial guards which is convex. Section 4 presents a procedure for deciding termination of loop program with polynomial guards. In Section 5, we show how to compute the transformation matrix symbolically to avoid floating point errors in computation. Finally, conclusions are given in Section 6.

2 Preliminaries

We use standard mathematical notation for representing vectors and matrices. Let $\mathcal{C}, \mathcal{R}$ and $\mathcal{Z}$ be the complex number field, real number field and integer number domain, respectively. An $(n \times n)$-matrix with constant entries a_{ij} at the (i, j)-position is denoted by $A = (a_{ij})$ where i, j denote indices ranging over integers. A diagonal matrix $A = (a_{ij}) = diag(\lambda_1, \cdots, \lambda_n)$ has $a_{ii} = \lambda_i$ and $a_{ij} = 0$ otherwise. In particular, an $(n \times 1)$ matrix is called a vector, and is denoted by $\mathbf{c}, \mathbf{d}$ whenever the components of the vector are known constants; and by $\mathbf{x}, \mathbf{y}$ whenever the components of the vector are all variables. The transpose of a matrix $A = (a_{ij})$ is denoted by A^T. Note that the transpose of a column vector $\mathbf{c}$ is a row vector $\mathbf{c}^T$. Using juxtaposition for matrix multiplication, we note that $\mathbf{c}^T\mathbf{d} = \sum_i c_i d_i$ denotes the inner product of the vectors $\mathbf{c}$ and $\mathbf{d}$.

We will also denote matrices by specifying the submatrices inside it. For instance, $diag(J_1, \cdots, J_n)$ would denote a matrix which has submatrices $J_1, \cdots, J_n$ on its "diagonal" and 0 elsewhere. If A is a $(n \times n)$-matrix and $\mathbf{c}$ is a vector such that $A\mathbf{c} = \lambda\mathbf{c}$, then $\mathbf{c}$ is called an eigenvector of A corresponding to the eigenvalue λ.

A function $f : \mathcal{R}^n \to \mathcal{R}$ is called a convex function if $f(\alpha\mathbf{x} + (1-\alpha)\mathbf{y}) \geq \alpha f(\mathbf{x}) + (1-\alpha)f(\mathbf{y})$ for any $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{R}^n$ and $0 \leq \alpha \leq 1$. A set S is convex if $\alpha\mathbf{u} + (1-\alpha)\mathbf{v} \in S$, for any $\mathbf{u}, \mathbf{v} \in S$.

Program executions can be carried through the various changes of configuration allowed by the program's transition relation. We say a program is terminating if all of its executions are finite. A program is called nonterminating if there exists at least one infinite execution.

We consider programs of the following form:

$$\texttt{P1}: \ \texttt{while} \ \ (f(\mathbf{x}) > 0) \ \ \{\mathbf{x} := A\mathbf{x} + \mathbf{c}\}.$$

where f is a polynomial defined on $\mathcal{R}^n$ and $\mathbf{c}$ is a nonzero vector. The assignment $x := A\mathbf{x} + \mathbf{c}$ is interpreted as being done simultaneously and not in any sequential

order. In the following discussion, we often consider its homogenous form $F(\bar{\mathbf{x}}) = x_0^{\deg(f)} f(\mathbf{x}/x_0)$ where $\bar{\mathbf{x}} = (x_1, \ldots, x_n, x_0) = (\mathbf{x}, x_0)$. Then $F(\mathbf{x}, 1) = f(\mathbf{x})$. According to the geometry theory, every positive degree homogenous equation $F(\bar{\mathbf{x}}) = 0$ defines a conical surface in an $n+1$ dimensional space with the origin as the apex.

3 Convex Guard

In this section, we will focus on polynomial guard which is convex. And the convexity will lead to some propositions for the program analysis.

3.1 Homogeneous Case

First let us consider a guard $F(\mathbf{x}) > 0$, where $F(\mathbf{x})$ is a homogenous polynomial in $x_0, x_1, \cdots, x_n$. We assume that F is irreducible. Then $F(\mathbf{x}) = 0$ defines an irreducible convex hypersurface. Since it is rigorous for a function to be convex globally, we often consider the function which is convex within a linear constraint $L(\mathbf{x}) > 0$ if needed. For simplicity, we set $F(\mathbf{x})$ is homogenous form firstly. Following these assumptions, a program can be written as

$$\texttt{Q1}:\texttt{while}\ \ (F(\mathbf{x}) > 0, L(\mathbf{x}) > 0)\ \ \{\mathbf{x} := A\mathbf{x}\},$$

where $F(\mathbf{x})$ is a homogenous polynomial with degree greater than one and $L(\mathbf{x})$ is a linear homogenous polynomial. $F(\mathbf{x})$ and $L(\mathbf{x})$ define a convex set, i.e., $F(\mathbf{x})$ is a convex function on $S = \{\mathbf{x} | F(\mathbf{x}) > 0, L(\mathbf{x}) > 0\}$. By the discussion in [15], we can obtain a similar theorem.

Theorem 1. *If the program* Q1 *defined by an* $(n \times n)$*-real matrix* A *is nonterminating then there exists a real eigenvector* $\mathbf{v}$ *of* A*, corresponding to a positive real eigenvalue* λ *such that* $F(\mathbf{v}) \geq 0$ *and* $L(\mathbf{v}) \geq 0$*.*

Proof. Suppose the Program Q1 is nonterminating. Define the set NT of all points on which the program does not terminate. $NT = \{\mathbf{x} \in \mathcal{R}^n | F(\mathbf{x}) > 0, L(\mathbf{x}) > 0, F(A\mathbf{x}) > 0, L(A\mathbf{x}) > 0, \cdots, F(A^i\mathbf{x}) > 0, L(A^i\mathbf{x}) > 0 \cdots\}$. By assumption, $NT \neq \emptyset$. The set NT is also A-invariant, that is, if $\mathbf{v} \in NT$, then $A\mathbf{v} \in NT$. Since $F(\mathbf{x}) > 0$ and $L(\mathbf{x}) > 0$ define a convex set and there are convex functions, the set NT is convex.

Define $T = \mathcal{R}^n - NT$ to be the set of all points where the program terminates. Define the boundary, ∂NT, of NT and T as the set of all $\mathbf{v}$ such that (for all ε) there exists a point in the ε-neighborhood of $\mathbf{v}$ that belongs to T and another that belongs to NT. Let NT' be the completion of NT, that is, $NT' = NT \cup \partial NT$. Since NT is A-invariant, it means that A maps NT into NT. By continuity we have that A also maps NT' into NT'. Now, NT' is convex, and if we identify points $\mathbf{x}$ and $\mathbf{y}$, written as $\mathbf{x} \sim \mathbf{y}$, that are positive scalar multiples of each other ($x = \lambda y$), then the resulting set $(NT'/\sim)$ is closed and bounded. By Brouwers fixed point theorem [18] and noting L is linear, it follows that there is a positive real eigenvector $\mathbf{v}$ of A in NT'. For all points $\mathbf{u} \in NT$, $F(\mathbf{u}) > 0$. By continuity, $F(\mathbf{v}) \geq 0$ and $L(\mathbf{v}) \geq 0$. □

Corollary 1. *If there is no real eigenvector* $\mathbf{v}$ *of* A *such that* $F(\mathbf{v})L(\mathbf{v}) = 0$*, then the loop* `Q1` *is nonterminating if and only if there exists a real eigenvector* $\mathbf{v}$ *on which the loop is nonterminating.*

Remark 1. For an eigenvalue λ of a matrix A, it has an eigenvector space $V = \{k\mathbf{v} | A\mathbf{v} = \lambda\mathbf{v}, k \in \mathcal{Z}\backslash 0\}$. Then $\mathbf{cv} \neq 0, \mathbf{v} \in V$ can be positive or negative according to the sign of k, so we should check $\mathbf{v}$ and $-\mathbf{v}$ following Corollary 1. The example 3 in [15] gave a wrong answer because the author only checked one of $\mathbf{v}$ and $-\mathbf{v}$.

Example 1. Consider the program:

$$\texttt{Q1}: \texttt{while}\ \ (-x^2 - y^2 + z^2/2 > 0, z > 0)\ \ \{(x, y, z)^T := A \cdot (x, y, z)^T\}.$$

where the assignment matrix is

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & -1 \\ \frac{1}{2} & 1 & \frac{1}{2} \end{pmatrix}.$$

The matrix A has three real eigenvalues as $-1, 1/2$ and 1, the corresponding eigenvectors are $(1, -2, 1)^T, (\frac{4}{7}, -\frac{2}{7}, 1)^T$ and $(1, 0, 1)^T$. One can check that there does not exist an eigenvector $\mathbf{v}$ such that $F(\mathbf{v}) = 0$. Then according to Corollary 1, this program is nonterminating, since the eigenvector $(\frac{4}{7}, -\frac{2}{7}, 1)$ is a nonterminating vector.

3.2 Nonhomogeneous Case

The restriction that $F(\mathbf{x})$ is of homogenous form is sometimes too restrictive. Fortunately, we can homogenize a generic polynomial $f(\mathbf{x})$ by adding a homogenizing variable x_0. The corresponding homogenous form is denoted by $F(\bar{\mathbf{x}})$. Similarly, the linear function of $L(\mathbf{x})$ is denoted by $L(\bar{\mathbf{x}})$.

Clearly the program `P1` is equivalent to the following homogenous form.

$$\texttt{P1}': \texttt{while}\ \ (F(\bar{\mathbf{x}}) > 0, x_0 > 0)\ \ \{\mathbf{x} := A\mathbf{x} + \mathbf{c}, x_0 := x_0\},$$

writing as the uniform form

$$\texttt{P1}': \texttt{while}\ \ (F(\bar{\mathbf{x}}) > 0, x_0 > 0)\ \ \{\bar{\mathbf{x}} := \bar{A}\bar{\mathbf{x}}\},$$

where $\bar{\mathbf{x}} = (\mathbf{x}, x_0)$ and $\bar{A} = \begin{pmatrix} A & \mathbf{c} \\ 0 & 1 \end{pmatrix}$.

Lemma 1. $f(\mathbf{x})$ *is a convex function on a set* S *if and only if* $F(\bar{\mathbf{x}})$ *is a convex function on* $\bar{S}$*, where* $\bar{\mathbf{x}} = (\mathbf{x}, x_0)$ *and* $\bar{S} = (S, x_0)$ *with* $x_0 > 0$.

Proof. One can check the lemma by the definition directly. □

Proposition 1. *The nonhomogeneous Program* `P1` *is nonterminating if and only if the homogenous Program* `P1'` *is nonterminating.*

Proof. Let $\mathbf{v}$ be a nonterminating vector of P1, then $\bar{\mathbf{v}} = (\mathbf{v}, 1)^T$ is a nonterminating vector of P1′. For the converse, if $\bar{\mathbf{v}} = (v_1, \ldots, v_n, v_0)^T$ is a nonterminating vector of P1′, then $v_0 > 0$. Therefore, $(v_1/v_0, \ldots, v_n/v_0)$ is a nonterminating vector of P1. □

According to this proposition and Lemma 1, it suffices to discuss the homogenous form in the following sections.

Theorem 2. *Suppose that $F(\bar{\mathbf{x}})$ is convex on $\{\mathbf{x}|F(\mathbf{x}) > 0, x_0 > 0\}$, if the program P1′ is nonterminating, then there exists a real eigenvector $\bar{\mathbf{v}}$ of $\bar{A}$, corresponding to a positive eigenvalue λ such that $F(\bar{\mathbf{v}}) \geq 0$ and $v_0 \geq 0$.*

Corollary 2. *If there is no real eigenvector $\bar{\mathbf{v}}$ of A such that $F(\bar{\mathbf{v}}) = 0$ or $v_0 = 0$, then the loop P1′ is nonterminating if and only if there exists an eigenvector $\mathbf{v}$ on which the loop is nonterminating.*

Since $\bar{A}$ is expanded from A, we obtain the following lemma.

Lemma 2. *Let $\bar{\mathbf{v}} = (v_1, \ldots, v_n, v_0)$ be an eigenvector of $\bar{A}$, then there is only one eigenvector such that $v_0 \neq 0$, corresponding to the eigenvalue($\lambda = 1$) of $\bar{A}$.*

Proof. The eigenvalues of $\bar{A}$ are the roots of the characteristic polynomial $C(\lambda) = \det(\bar{A} - \lambda I_{n+1}) = 0$. However $C(\lambda) = (\lambda - 1)\det(A - \lambda I_n)$, that means the eigenvalues of $\bar{A}$ are formed by the eigenvalues of A and $\lambda = 1$. Let $\mathbf{v}$ be an eigenvector of A, then we can verify that $(\mathbf{v}, 0)^T$ is a eigenvector of $\bar{A}$. Hence, we only need to find the eigenvector corresponding to $\lambda = 1$. This eigenvector is a solution of the linear system $(A - I_n)\mathbf{v} = -\mathbf{c}v_0$, there always exists a solution which is decided by A and $\mathbf{c}$ with $v_0 \neq 0$. This is the unique eigenvector of $\bar{A}$ following the lemma. □

Since $x_0 > 0$ is a guard, according to Lemma 2 and Corollary 2, we only need to check this vector for the guard $F(\bar{\mathbf{v}})$. Where $\bar{\mathbf{v}} = (\mathbf{v}, 1)$, with $\mathbf{v}$ a solution of $(A - I_n)\mathbf{v} = -\mathbf{c}$(setting $v_0 = 1$).

Corollary 3. *Let $\bar{\mathbf{v}}$ be the unique eigenvector of $\bar{A}$ mentioned in Lemma 2. Then the loop P1′ is nonterminating if and only if $F(\bar{\mathbf{v}}) > 0$.*

Example 2. Consider the program:

$$\texttt{P1}: \texttt{while}\ \ (-x^2 - y^2 + 4 > 0)\ \ \{x := x - y + 1; y := x + y - 1\}.$$

Then its homogenous form is

$$\texttt{P1}': \texttt{while}\ \ (-x^2 - y^2 + 4z^2 > 0, z > 0)\ \ \{x := x - y + z; y := x + y - z; z := z\}.$$

The guards define a convex cone set and the assignment matrix is

$$\bar{A} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

$\bar{A}$ only has one real eigenvalue $\lambda = 1$ and the corresponding vector is $\bar{\mathbf{v}} = (1, 1, 1)^T$. Since $F(\bar{\mathbf{v}}) = 2 > 0$, according to Corollary 2, we only need to check whether $\mathbf{v}$ is a

terminating point or not. By the proof of Theorem 1, we find that $\bar{\mathbf{v}}$ is fix point of NT, then it is a nonterminating point. Therefore, P1′ is nonterminating, and as a sequence, P1 is nonterminating with a point $(1,1)^T$.

We can also consider this example on the other hand, the matrix A has no real eigenvalues, according to Corollary 3, we solve $(A - I_n)\mathbf{v} = -\mathbf{c}$, that is

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mathbf{v} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

Then $\mathbf{v} = (1,1)^T$ is a solution, and we have shown that it is a nonterminating point.

4 Program Simplification

According to Section 3, it is shown that Q1 does not terminate if we find an eigenvector $\mathbf{v}$ associated to a positive eigenvalue to be a nonterminating vector. However, it is not decided when there exist eigenvectors satisfying $F(\mathbf{v}) = 0$ or $L(\mathbf{v}) = 0$. Furthermore, the guards may not be convex if the guard $L(\mathbf{v})$ is not linear. And we need to give more discussion of the program in this section.

Consider the effect of repeated linear assignments $(\mathbf{x} := A\mathbf{x})$, it will be much simpler if A is a diagonal matrix. So we try to diagonalize the assignment matrix A. It is well known that it can be transformed to its Jordan canonical form which is the simplest equivalent form. We recall the proposition which can found in many linear algebra books such as [19].

Proposition 2. *For any square matrix A, there is an invertible matrix P, and a matrix D such that $D = P^{-1}AP$. Here $D = diag(J_1, J_2, \cdots, J_K)$ is the real Jordan form with each block J_i having either of the two forms:*

$$\begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \dots & \lambda_i \end{pmatrix}, \quad \begin{pmatrix} D_i & I & 0 & \dots & 0 \\ 0 & D_i & I & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & I \\ 0 & 0 & 0 & \dots & D_i \end{pmatrix}, \tag{1}$$

where λ_i is a real eigenvalue of A and D_i is a real 2×2 matrix as $\begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$ associated to a pair of conjugate eigenvalues $a_i \pm b_i\mathrm{i}$, $\mathrm{i}^2 = -1$.

For uniformity, we denote the Jordan block only as the second form. Then the first form is the degenerate case that D_i and I are both 1×1 matrices and we treat it as a real. And the modular $|D_i|$ is defined as $|\lambda_i|$ and $\sqrt{a_i^2 + b_i^2}$ for the two cases respectively.

We now see that symbolically powering the matrix A is an essential step in deciding termination of the loop. If $D = P^{-1}AP$ then $D^n = (P^{-1}AP)^n = P^{-1}A^nP$. Hence powering the matrix A is simplified as powering the matrix D. Since P is invertible, we can get the following proposition.

Proposition 3. *Let P be an invertible linear transformation. The program*

$$\texttt{Q1} : \texttt{while}(F(\mathbf{x}) > 0, L(\mathbf{x}) > 0) \ \ \{\mathbf{x} := A\mathbf{x}\}.$$

is terminating if and only if the program

$$\texttt{Q2} : \texttt{while}(F(P\mathbf{y}) > 0, L(P\mathbf{y}) > 0) \ \ \{\mathbf{y} := P^{-1}AP\mathbf{y}\}$$

is terminating.

Suppose the invertible transformation P is given, we then write the program Q2 as

$$\texttt{Q3} : \texttt{while}(F(\mathbf{y}) > 0, L(\mathbf{y}) > 0) \ \ \{\mathbf{y} := D\mathbf{y}\}$$

Here, we still write F and L for less symbols. According to the structure of D, we partition the variables in $\mathbf{y}$ into $\mathbf{y}_1, \ldots, \mathbf{y}_K$ and rewrite Q3 as

$$\texttt{Q3} : \texttt{while}(F(\mathbf{y}_1, \ldots, \mathbf{y}_K) > 0, L(\mathbf{y}_1, \ldots, \mathbf{y}_K) > 0)$$

$$\{\mathbf{y}_1 := J_1\mathbf{y}_1; \ldots; \mathbf{y}_K = J_K\mathbf{y}_K\}.$$

If $F(\mathbf{x})$ is also linear, the following Lemma 1 in [15], the program can be reduced to considering the Jordan blocks only corresponding to the positive eigenvalues. However, it does not hold when $F(\mathbf{x})$ is nonlinear. For a simple instance, $(D_1D_2^2D_3^4)^N$ is positive for any number N of iteration, where $D_1 = 2, D_2 = -3$ and $D_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ correspond to positive, negative and complex eigenvalues respectively.

For an input $\mathbf{v}$, we now consider loop conditions at the N-th iteration. Assume that $\mathbf{y}_i$ assigned of $\mathbf{v}_i$ by A has K_i components, $\mathbf{y}_{i_0}, \mathbf{y}_{i_1}, \ldots, \mathbf{y}_{i_{K_i-1}}$, where each $\mathbf{y}_{i_k}$ is either a 2×1 or 1×1 matrix depending on the choice of D_i. Then the value of $\mathbf{y}_i$ at the N-th iteration is given by

$$\mathbf{y}_i(N) = J_i^N\mathbf{v}_i = \begin{pmatrix} D_i^N & ND_i^{N-1} & \binom{N}{2}ND_i^{N-2} & \cdots & \binom{N}{K_i-1}D_i^{N-(K_i-1)} \\ 0 & D_i^N & ND_i^{N-1} & \cdots & \binom{N}{K_i-2}D_i^{N-(K_i-2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & D_i^N & ND_i^{N-1} \\ 0 & 0 & \cdots & 0 & D_i^N \end{pmatrix} \mathbf{v}_i. \quad (2)$$

If $D_i \in \mathcal{R}$, then one can check that

$$\lim_{N\to\infty} \frac{\binom{N}{k-1}D_i^{N-(k-1)}}{\binom{N}{k}D_i^{N-k}} = 0. \quad (3)$$

If $D_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$, we rewrite it as $D_i = \sqrt{a_i^2 + b_i^2}\begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$ where $\theta_i = \arccos(\frac{a_i}{\sqrt{a_i^2+b_i^2}})$. Then $D_i^k = |D_i|^k \begin{pmatrix} \cos(k\theta_i) & -\sin(k\theta_i) \\ \sin(k\theta_i) & \cos(k\theta_i) \end{pmatrix}$ for any $k \in \mathcal{Z}^+$ and

$$\lim_{N\to\infty} \frac{|\binom{N}{k-1}D_i^{N-(k-1)}|}{|\binom{N}{k}D_i^{N-k}|} = 0. \quad (4)$$

Consider one homogenous term of $F(\mathbf{y})$ as $\mathbf{y}_1^{m_1}\mathbf{y}_2^{m_2}\cdots\mathbf{y}_K^{m_K}$ where $\sum_{i=1}^{K} m_i = m$. In the expression $\mathbf{y}_i^{m_i} = \mathbf{y}_{i_0}^{m_{i_0}}\mathbf{y}_{i_1}^{m_{i_1}}\cdots\mathbf{y}_{i_{K_i-1}}^{m_{i_{K_i-1}}}$ where $\sum_{j=0}^{K_i-1} m_{i_j} = m_i$ and if $\mathbf{y}_{i_k}$ is 2×1 then $\mathbf{y}_{i_j}^{m_{i_j}} = y_{i_{j_1}}^{m_{i_{j_1}}} y_{i_{j_2}}^{m_{i_{j_2}}}$ where $m_{i_{j_1}} + m_{i_{j_2}} = m_{i_j}$.

By (3), (4) and the equation (2), if $\mathbf{y}_{i_j}$ is 1×1 then $\mathbf{y}_i^{m_i} = (J_i^N[1]\cdot\mathbf{v}_i)^{m_{i_0}}(J_i^N[2]\cdot\mathbf{v}_i)^{m_{i_1}}\cdots(J_i^N[K_i]\cdot\mathbf{v}_i)^{m_{i_{K_i-1}}}$ is dominated by

$$\lfloor\mathbf{y}_i^{m_i}\rfloor = (J_i^N[1,K_i]\cdot\mathbf{v}_{i,K_i})^{m_{i_0}}(J_i^N[2,K_i]\cdot\mathbf{v}_{i,K_i})^{m_{i_1}}\cdots(J_i^N[K_i,K_i]\cdot\mathbf{v}_{i,K_i})^{m_{i_{K_i-1}}} \tag{5}$$

when N is large enough, where $J_i^N[j]$ is the j-th row vector of J_i^N, $J_i^N[j,K_i]$ is K_i-th element of the vector and $\mathbf{v}_{i,K_i}$ is K_i-th element of the vector $\mathbf{v}_i$.

If $\mathbf{y}_{i_j}$ is 2×1, then the dominating term of $\mathbf{y}_i^{m_i}$ is

$$\lfloor\mathbf{y}_i^{m_i}\rfloor = (J_i^N[1,K_i]\cdot\mathbf{v}_{i,K_i})^{m_{i_0}}(J_i^N[2,K_i]\cdot\mathbf{v}_{i,K_i})^{m_{i_1}}\cdots(J_i^N[K_i,K_i]\cdot\mathbf{v}_{i,K_i})^{m_{i_{K_i-1}}},$$

where $\mathbf{v}_{i,l} = (\mathbf{v}_{i,l_1}, \mathbf{v}_{i,l_2})$. Precisely, $(J_i^N[1,K_i]\cdot\mathbf{v}_{i_{K_i}})^{m_{i_0}}$ can be expanded as

$$\begin{aligned}&(\tbinom{N}{K_i-1}|D_i|^{N-K_i-1})^{m_{i_0}}\\ &\cdot((\mathbf{v}_{i,K_{i_1}}\cos((N-(K_i-1))\theta_i) - \mathbf{v}_{i,K_{i_2}}\sin((N-(K_i-1))\theta_i))^{m_{i_{0_1}}}\\ &\cdot((\mathbf{v}_{i,K_{i_1}}\cos((N-(K_i-1))\theta_i) + \mathbf{v}_{i,K_{i_2}}\sin((N-(K_i-1))\theta_i))^{m_{i_{0_2}}},\end{aligned} \tag{6}$$

and similar to the other terms.

Therefore, if N is large enough, then the homogenous item $\mathbf{y}_1^{m_1}\mathbf{y}_2^{m_2}\cdots\mathbf{y}_K^{m_K}$ of F is dominated by the product of their dominating term $\lfloor\mathbf{y}_1^{m_1}\rfloor\lfloor\mathbf{y}_2^{m_2}\rfloor\cdots\lfloor\mathbf{y}_K^{m_K}\rfloor$.

The value of variables in y_i, after the N-th iteration, are given by equation (2). As before, assume that the N-th the loop condition is written as $F(\mathbf{y}_1,\ldots,\mathbf{y}_K) > 0$. We can express the requirement that the loop condition be true after the N-th iteration as

$$F(\mathbf{y}_1(N),\ldots,\mathbf{y}_K(N)) > 0.$$

Without loss of generality, we assume that $0 \le |D_1| \le |D_2| \le \cdots \le |D_K|$. Considering the equation using determined terms, we then can write F as $F(\mathbf{S})$, where $\mathbf{S} := \{(D_1)^N,\cdots,\tbinom{N}{K_1}D_1^{N-(K_1-1)},\cdots,(D_K)^N,\cdots,\tbinom{N}{K_k}D_i^{N-(K_k-1)}\}$ is the set being regarded as main variables. If F is homogenous with degree m, then the homogenous item set spanned by $\mathbf{S}$ with degree m is

$$\mathbf{S}^m = \{S = \prod_{\sum m_i = m} s_i^{m_i} | s_i \in \mathbf{S}\}.$$

Suppose N is large enough, we can sort the elements of $\mathbf{S}^m$ by their absolute values, and only one is kept if it has other same absolute value elements. Then we can simplify $\mathbf{S}^m = \{|S_1| > |S_2| \cdots > |S_l|\}$. According to $\mathbf{S}^m$, F can be rearranged by the value order as

$$F(N,\mathbf{v}) = f_1(N,\mathbf{v})\cdot|S_1| + \cdots + f_l(N,\mathbf{v})\cdot|S_l| \tag{7}$$

where $\mathbf{v}$ is the initial input $\mathbf{y}(0)$, the coefficients of polynomials $f_i(N,\mathbf{v})$ are formed by the coefficients of (5) and (6). So N can only be in $\cos((N-(K_i-1))\theta_i)$ and

$\sin((N-(K_i-1))\theta_i)$ as (6), which always induces a rotated value corresponding to $2\times 2-D_i$. Hence, we can write the coefficient function as

$$f_i(N,\mathbf{v}) = f_i(\mathbf{v}, \cos((N-N_{i_1})\theta_{i_1}), \sin((N-N_{i_1})\theta_{i_1}), \cdots, \cos((N-N_{i_k})\theta_{i_k}), \sin((N-N_{i_k})\theta_{i_k})), \tag{8}$$

where k is the number of the complex eigenvalues.

Now, we decide the termination of program Q1. For the loop condition (7), we can consider the coefficients of equation $F(\mathbf{S})$. Intuitively if $\mathbf{y}(0)$ is a witness to nontermination, then $f_i(N,\mathbf{y}(0))>0$ and $f_j(N,\mathbf{y}(0))=0$ for all $0\le j<i$ and $N>N_0\ge 0$. Then we write the functions in a semi-algebraic system(SAS) as

$$\mathcal{S}_i = \{\mathbf{v}|f_i(N,\mathbf{v}))>0, f_j(N,\mathbf{v})=0, 0\le j<i, N>N_0\}.$$

That means we need to solve an SAS to decide the termination after the simplification. Since the guard (7) has finite items, it can only induce SASs as $\mathcal{S}_i, i=1,\ldots,l$.

And we then get the following theorem.

Theorem 3. *The termination of*

$$\texttt{Q1}:\texttt{while}\ \ (F(\mathbf{x})>0, L(\mathbf{x})>0)\ \ \{\mathbf{x}:=A\mathbf{x}\},$$

is decidable if and only if the SASs $\mathcal{S}_i, i=1,\ldots,l$ are solvable.

Remark 2. Here *solvable* means that we can decide whether an SAS has real solutions or not.

If there exists $\mathbf{v}_0$ satisfies a SAS $\mathcal{S}_i$ for $N>N_0$, then $\mathbf{v}_0$ is a nonterminating point and the program is nonterminating. The solvablity of the SAS depends on the number of its functions. If it only has finite functions then it is solvable. The number of functions can also be infinite with N increasing. However, the situation is easy if the functions in the SAS are integer periodic functions. This situation can happen where the normalized complex eigenvalues are all integer periodic, i.e., $\theta_i=\frac{p}{q}\pi, p,q\in\mathcal{Z}$. Since the functions in the SAS are periodic, assuming $\tilde{N}$ being the common period, then we only need to consider the functions of SAS in a period and it is formed with finite functions

$$\mathcal{S}_i = \{\mathbf{v}|f_i(N,\mathbf{v}))>0, f_j(N,\mathbf{v})=0, 0\le j<i, N_0+\tilde{N}>N>N_0\}.$$

And this SAS is solvable. We summarize this situation as a corollary.

Corollary 4. *If all the normalized complex eigenvalues are integer periodic, then the termination of*

$$\texttt{Q1}:\texttt{while}\ \ (F(\mathbf{x})>0, L(\mathbf{x})>0)\ \ \{\mathbf{x}:=A\mathbf{x}\}$$

is decidable.

Example 3. Consider the program

$$\texttt{Q1}:\texttt{while}\ \ (-x^2+10y^2+z^2>0, x>0)\ \ \{x:=2y+z; y:=-x+z; z:=y+z\}$$

The assignment matrix is

$$A = \begin{pmatrix} 0 & 2 & 1 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

The set defined by the guards is not convex and the results in Section 3 can not work for this example. We now analysis using the above procedure. The real Jordan form of A is J and the corresponding transformation matrix is P.

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, P = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}.$$

The new program is

$$\texttt{Q2}: \texttt{while}\ \ (F_1 := 9x_2^2+7x_3^2-2x_1x_2-2x_1x_3-24x_2x_3 > 0, F_2 := x_1+x_2+2x_3 > 0)$$

$$\{x_1 := x_1; x_2 := -x_3; x_3 := x_2\}$$

The general solution is given by

$$x_1(N) = 1^N x_1(0)$$
$$\begin{pmatrix} x_2(N) \\ x_3(N) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^N \begin{pmatrix} x_2(0) \\ x_3(0) \end{pmatrix} = 1^N \cdot \begin{pmatrix} \cos(\frac{N\pi}{2}) & -\sin(\frac{N\pi}{2}) \\ \sin(\frac{N\pi}{2}) & \cos(\frac{N\pi}{2}) \end{pmatrix} \begin{pmatrix} x_2(0) \\ x_3(0) \end{pmatrix}$$

The first loop condition corresponding to the loop condition F_1 is

$$1^{2N} \cdot \big(9x_3^2 + 7x_2^2 + 24x_2x_3 + \cos(\tfrac{N\pi}{2}) \cdot (-2x_1x_2 - 2x_1x_3) + \sin(\tfrac{N\pi}{2}) \cdot (2x_1x_3 - 2x_1x_2) + \cos(\tfrac{N\pi}{2})^2 \cdot (2x_2^2 - 2x_3^2 - 48x_2x_3)\big) > 0$$

and the second loop condition F_2 is $x_1+\cos(\frac{N\pi}{2})\cdot(x_2+2x_3)+\sin(\frac{N\pi}{2})\cdot(2x_2-x_3) > 0$.

In many cases, one can find that all the items are the dominant items. We now check the conditions for a period $N = 4n, 4n+1, 4n+2$ and $4n+3, n \in \mathcal{Z}^+$. Then the generated constraints of the loop conditions are the following, respectively,

$$\begin{aligned} Con_1 &:= \{9x_2^2 + 7x_3^2 - 2x_1x_2 - 2x_1x_3 - 24x_2x_3 > 0, x_1 + x_2 + 2x_3 > 0\}, \\ Con_2 &:= \{7x_2^2 + 9x_3^2 - 2x_1x_2 + 2x_1x_3 + 24x_2x_3 > 0, x_1 + 2x_2 - x_3 > 0\}, \\ Con_3 &:= \{9x_2^2 + 7x_3^2 + 2x_1x_2 + 2x_1x_3 - 24x_2x_3 > 0, x_1 - x_2 - 2x_3 > 0\}, \\ Con_4 &:= \{7x_2^2 + 9x_3^2 + 2x_1x_2 - 2x_1x_3 + 24x_2x_3 > 0, x_1 - 2x_2 - x_3 > 0\}. \end{aligned}$$

Then the nonterminating points is in the set $Con := \bigcap_{i=1}^{4} Con_i$ and Q2 is nonterminating if Con is not empty.

In fact, this set is not empty since we can check that $(x_1, x_2, x_3) = (5, 2, 0)$ is a point of Con and it makes Program Q2 nonterminating, and correspondingly, the point $x = -\frac{3}{2}, y = \frac{7}{2}, z = \frac{3}{2}$ makes Program Q1 nonterminating.

If we consider the Jordan blocks only corresponding to the positive eigenvalue, such as Lemma 1 in [15]. From Q2, we get

$$\texttt{Q3}: \texttt{while}\ \ (-4x_1 > 0, x_1 > 0)\ \ \{x_1 := x_1\}.$$

Obviously, the program Q3 is terminating, and correspondingly the program Q1 is terminating. However, the program Q1 is nonterminating. Hence, we need to consider the Jordan blocks corresponding to the positive, negative, and complex eigenvalues respectively.

Actually, the above procedure is a generalization of the rusult in [15]. Tiwari gave the subtle discussion for this situation showing that the nonterminating points can only be in the SASs whose functions involve the positive eigenvalues. That means these functions are without N as the variable. Then the SASs are solvable since the number of functions is finite. We write the result of [15] as a corollary.

Corollary 5. *If the guards of program*

$$\texttt{Q1}: \texttt{while}\ \ (F(\mathbf{x}) > 0, L(\mathbf{x}) > 0)\ \ \{\mathbf{x} := A\mathbf{x}\}$$

are linear, then the termination of Q1 *is decidable.*

4.1 General Polynomial Guard

We find that the convexity of F leads to some interesting properties and advantages in Section 3, but it is not necessary for the simplification in this section. On the other hand, the number of guard polynomials dose not change the difficulty of solving the SAS in Section 4 theoretically.

Consider the general case:

$$\texttt{P}: \texttt{while}\ \ (f_1(\mathbf{x}) > 0, \ldots, f_l(\mathbf{x}) > 0)\ \ \{\mathbf{x} := A\mathbf{x} + \mathbf{c}\}.$$

It has two cases with homogenous form. If $\mathbf{c} \neq 0$ or some $f_i(\mathbf{x})$ is nonhomogeneous, it is equivalent to

$$\texttt{Q}: \texttt{while}\ \ (F_1(\bar{\mathbf{x}}) > 0, \ldots, F_l(\bar{\mathbf{x}}) > 0, x_0 > 0)\ \ \{\bar{\mathbf{x}} := \bar{A}\bar{\mathbf{x}}\}.$$

If $\mathbf{c} = 0$ and all $f_i(\mathbf{x})$ are homogenous, then P can be written as

$$\texttt{P}': \texttt{while}\ \ (F_1(\mathbf{x}) > 0, \ldots, F_l(\mathbf{x}) > 0)\ \ \{\mathbf{x} := Ax\}.$$

The termination is decidable for the two situations according to Corollary 4 and Corollary 5. The generic case is to consider the program without any assumptions is depended on the solvableness of SASs and there are not obvious results. Recently, Xia and Zhang [20] proposed a conjecture that the decision of P′ is undecidable using another technique.

5 Computing the Transformation Matrix

The termination can be determined following the discussion in Sections 3 and 4. Then the main task is to find the transformation matrix P of A such that $P^{-1}AP = D$ where D is the real Jordan form. P is formed by eigenvectors and generalized eigenvectors

of A and there are several numerical algorithms to compute these eigenvectors. Here we give a sketch of the computation. Let D_i be a real eigenvalue $D_i = \lambda_i$ or a matrix corresponding to a pair of conjugate eigenvalues $a_i \pm b_i\mathrm{i}$, whose associated Jordan block is as the form of (1). We call $\mathbf{v}$ a generalized eigenvector of λ_i with order K if $(A - \lambda_i I)^K \mathbf{v} = 0$ but $(A - \lambda_i I)^{K-1}\mathbf{v} \neq 0$. There exists a K_i-th order generalized eigenvector associated to the Jordan block J_i. Let

$$\mathbf{v}_1 = \mathbf{v};\ \mathbf{v}_2 = (A - \lambda_i I)\mathbf{v}_1;\ \ldots; \mathbf{v}_{K_i} = (A - \lambda_i I)\mathbf{v}_{K_i - 1}, \mathbf{v}_j \in \mathcal{R}^n$$

be a chain of the generalized eigenvectors and $\mathbf{v}_1$ the K_i-th order generalized eigenvector, then we have

$$A(\mathbf{v}_{K_i}|\mathbf{v}_{K_{i-1}}|\cdots|\mathbf{v}_2|\mathbf{v}_1) = (\mathbf{v}_{K_i}|\mathbf{v}_{K_{i-1}}|\cdots|\mathbf{v}_2|\mathbf{v}_1)J_i,$$

and we denote the matrix $(\mathbf{v}_{K_i}|\mathbf{v}_{K_{i-1}}|\cdots|\mathbf{v}_2|\mathbf{v}_1)$ by P_i. It is obvious that $\mathbf{v}_{K_i}$ is an eigenvector of A.

If $D_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$, similarly, we can get an eigenvectors chain in complex space

$$\mathbf{v}_1 = \mathbf{v}; \mathbf{v}_2 = (A - \lambda_i I)\mathbf{v}_1;\ \ldots;\ \mathbf{v}_{K_i} = (A - \lambda_i I)\mathbf{v}_{K_i - 1}, \mathbf{v}_i \in \mathcal{C}^n, \lambda_i = a_i + b_i\mathrm{i}.$$

Since $\mathbf{v}_i \in \mathcal{C}^n$, we can decompose them as $\mathbf{v}_i = \mathbf{x}_i + \mathbf{y}_i\mathrm{i}$, that is,

$$\mathbf{v}_1 = \mathbf{x}_1 + \mathbf{y}_1\mathrm{i};\ \mathbf{v}_2 = \mathbf{x}_2 + \mathbf{y}_2\mathrm{i};\ \cdots;\ \mathbf{v}_{K_i} = \mathbf{x}_{K_i} + \mathbf{y}_{K_i}\mathrm{i}.$$

Then we have the following equations, posed in two different ways:

$$\begin{array}{r|l} A\mathbf{v}_1 = \lambda_i\mathbf{v}_1 + \mathbf{v}_2 & A\mathbf{x}_1 = a_i\mathbf{x}_1 - b_i\mathbf{y}_1 + \mathbf{x}_2 \\ & A\mathbf{y}_1 = b_i\mathbf{x}_1 + a_i\mathbf{y}_1 + \mathbf{y}_2 \\ \vdots & \vdots \\ A\mathbf{v}_{K_i} = \lambda_i\mathbf{v}_{K_i} & A\mathbf{x}_{K_i} = a_i\mathbf{x}_{K_i} - b_i\mathbf{y}_{K_i} \\ & A\mathbf{y}_{K_i} = b_i\mathbf{x}_{K_i} + a_i\mathbf{y}_{K_i}. \end{array} \tag{9}$$

Then in matrix we have

$$A(\mathbf{y}_{K_i}|\mathbf{x}_{K_i}|\mathbf{y}_{K_{i-1}}|\mathbf{x}_{K_{i-1}}|\cdots|\mathbf{y}_1|\mathbf{x}_1) = (\mathbf{y}_{K_i}|\mathbf{x}_{K_i}|\mathbf{y}_{K_{i-1}}|\mathbf{x}_{K_{i-1}}|\cdots|\mathbf{y}_1|\mathbf{x}_1)J_i,$$

and we still denote $(\mathbf{y}_{K_i}|\mathbf{x}_{K_i}|\mathbf{y}_{K_{i-1}}|\mathbf{x}_{K_{i-1}}|\cdots|\mathbf{y}_1|\mathbf{x}_1)$ by P_i. Hence $P^{-1}AP = D$ where $P = (P_1|P_2|\cdots|P_K)$.

The subtle details of the numerical algorithms can be found in Linear Algebra Notes of MP274 Lecture Notes 1991 and the course files on *http://www.numbertheory.org/courses/MP274/*.

Although we can get the Jordan matrix D, the precision of the numerical computation relies on the manufactured presetting. In general cases, it is difficult to preset the precision for an unknown problem.

5.1 Computing the Transformation Matrix Symbolically

Since it is not safe to compute the transformation matrix numerically, we try to give transformation matrix in a symbolic way. Firstly, to avoid the numerical step in eigenvalues computation, the eigenvectors are solved from linear equations with the algebra conditions of eigenvalues. Secondly, we compute the generalized eigenvectors and construct the chain of generalized eigenvectors which are corresponding to Jordan blocks. For the real eigenvalues λ_i, the algebra condition equation is the characteristic polynomial $C(\lambda) = 0$. For a pair of conjugate eigenvalue $a \pm b\mathfrak{i}, b \neq 0$, we have $C(a \pm b\mathfrak{i}) = CR(a,b) + CI(a,b)\mathfrak{i} = 0$, then the algebraic condition equations are $CR(a,b) = 0, CI(a,b) = 0, b \neq 0$.

In the computation, we often factorize $C(\lambda) = C_1(\lambda) \cdots C_k(\lambda)$ in rational polynomial space $\mathcal{Q}[\lambda]$ and compute the chain of generalized eigenvectors for each different factor $C_i(\lambda)$. For the uniformity, we set the eigenvalue to be the form of $a \pm b\mathfrak{i}$ which is real for $b = 0$ and imaginary for $b \neq 0$. Then we need to solve the equations (9) with $CR(a,b) = 0, CI(a,b) = 0$. If $b = 0$ then the right-hand side of the equation system (9) defines two same equation systems for $\mathbf{x}$ and $\mathbf{y}$. In this case, there are two same chains of generator vectors and we only take one.

Alogrithm 1. *Computing the transformation matrix symbolically.*

step1. Compute and factorize the characteristic polynomial $C(\lambda) = C_1(\lambda) \cdots C_l(\lambda)$ *in rational polynomial space. For each square-free factor of* $C_k(\lambda)$*, compute* $CR(a,b) = 0$ *and* $CI(a,b) = 0$.

step2. Solve the linear systems (9) *with a pair of algebraic condition equations* $CR(a,b) = 0$ *and* $CI(a,b) = 0$.

step2.1 Solve the eigenvector $\mathbf{x}_i$ *and* $\mathbf{y}_i, i = 1, \ldots, e_i$ *from* $A\mathbf{x} = a\mathbf{x} - b\mathbf{y}, A\mathbf{y} = b\mathbf{x} + a\mathbf{y}$ *with* $CR(a,b) = 0$ *and* $CI(a,b) = 0$.

step2.2 If there exist, find the generalized eigenvectors $\mathbf{x}_{ij_i}$ *and* $\mathbf{y}_{ij_i}$ *from* $A\mathbf{x}_{i+1} = a\mathbf{x}_{i+1} - b\mathbf{y}_{i+1} + \mathbf{x}_i, A\mathbf{y}_{i+1} = b\mathbf{x}_{i+1} + a\mathbf{y}_{i+1} + \mathbf{y}_i$ *with* $CR(a,b) = 0$ *and* $CI(a,b) = 0$.

step2.3 Let $P_{ij_i} = (\mathbf{x}_{i1}|\mathbf{y}_{i1}|\cdots|\mathbf{x}_{ij_i}|\mathbf{y}_{ij_i})$ *and* $P_k = (P_{1j_1}|\cdots|P_{e_ij_{e_i}})$*, drop the linear dependent columns from* P_k.

step3. Output $P = (P_1|\cdots|P_l)$ *as the transformation matrix whose entries are symbolic with algebraic conditions.*

In the algorithm, l is often lesser than the number of Jordan blocks. Because P_k can represent several eigenvectors associated to different roots of algebraic conditions.

Example 4. Let A be the follow matrix,

$$A = \begin{pmatrix} 0&0&0&0&0&-27 \\ 1&0&0&0&0&18 \\ 0&1&0&0&0&9 \\ 0&0&1&0&0&-12 \\ 0&0&0&1&0&3 \\ 0&0&0&0&1&2 \end{pmatrix}. (\mathbf{y}_{11}|\mathbf{x}_{11}) = \begin{pmatrix} 18\,b & 9 \\ -9\,b & 9 \\ -12\,b & -6 \\ 6\,b & -6 \\ 2\,b & 1 \\ -b & 1 \end{pmatrix}, (\mathbf{x}_{22}|\mathbf{x}_{21}) = \begin{pmatrix} -9\,a & 9-9\,a \\ -9+6\,a & -15+12\,a \\ 6 & 12-4\,a \\ -2\,a & -2 \\ a-2 & a-1 \\ 1 & 1 \end{pmatrix}. \tag{10}$$

then its characteristic polynomial is $C(\lambda) = (\lambda^2 - 2\lambda + 3)(\lambda^2 - 3)^2$, the square-free factors are $(\lambda^2 - 2\lambda + 3)$ and $(\lambda^2 - 3)$. Their algebraic conditions are $CRI_1 = \{(a, b) \in \mathcal{R}^2 | a^2 - b^2 - 2a + 3 = 0, 2ab - 2b = 0\}$ and $CRI_2 = \{(a, b) \in \mathcal{R}^2 | a^2 - b^2 - 3 = 0, 2ab = 0\}$.

Using the above algorithm, we compute the corresponding (generalized)eigenvectors $(\mathbf{y}_{11}|\mathbf{x}_{11})$ with $(a, b) \in CRI_1$ and $(\mathbf{x}_{22}|\mathbf{x}_{21})$ with $(a, b) \in CRI_2$ in (10). We can find that $(\mathbf{x}_{22}|\mathbf{x}_{21})_{(a,b)\in CRI_2}$ implies two vector sets since CRI_2 has two real solutions $\{a = \pm\sqrt{3}, b = 0\}$. Then the transforation matrix is $P = (\mathbf{y}_{11}|\mathbf{x}_{11}|\mathbf{x}_{22}|\mathbf{x}_{21}|\mathbf{x}'_{22}|\mathbf{x}'_{21})$.

Then the Jordan form can be deduced by $P^{-1}AP$ within the algebraic equations $(a_1, b_1) \in CRI_1$, and $(a_2, b_2) \neq (a'_2, b'_2) \in CRI_2$.

$$P^{-1}AP = \begin{pmatrix} 1 & -2\,{b_1}^{-1} & 0 & 0 & 0 & 0 \\ b_1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{a'_2 a_2 - 3}{-a_2 + a'_2} & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{a'_2 a_2 - 3}{-a + a'_2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-a'_2 a_2 + 3}{-a_2 + a'_2} & 1 \\ 0 & 0 & 0 & 0 & 0 & \frac{-a'_2 a_2 + 3}{-a_2 + a'_2} \end{pmatrix}.$$

6 Conclusions

In this paper, observing only the eigenvectors (and the generalized eigenspace) corresponding to eigenvalues of the assignment matrix, we presented a technique to prove termination of single-path loop programs with polynomial guards and linear assignments. And we presented a decidable situation for the functions in the SASs are integer periodic. The symbolic technique is introduced to avoid floating point errors in computation. For the generic program, we will give further discussion, for instance, by considering the rational dependence of the complex eigenvalues.

References

1. Floyd, R.W.: Assigning meanings to programs. In: Schwartz, J.T. (ed.) Mathematical Aspects of Computer Science. Proceedings of Symposia in Applied Mathematics, vol. 19, pp. 19–32. American Mathematical Socity (1967)
2. Hoare, C.A.R.: An axiomatic basis for computer programming. Communications of ACM 12(10), 576–580 (1969)
3. Turing, A.: On computable numbers, with an application to the entscheidungsproblem. London Mathematical Socity 42(2), 230–265 (1936)
4. Colón, M., Sipma, H.: Synthesis of linear ranking functions. In: Margaria, T., Yi, W. (eds.) TACAS 2001. LNCS, vol. 2031, pp. 67–81. Springer, Heidelberg (2001)
5. Colón, M., Sipma, H.: Practical methods for proving program termination. In: Brinksma, E., Larsen, K.G. (eds.) CAV 2002. LNCS, vol. 2404, pp. 442–454. Springer, Heidelberg (2002)
6. Podelski, A., Rybalchenko, A.: A complete method for the synthesis of linear ranking functions. In: Steffen, B., Levi, G. (eds.) VMCAI 2004. LNCS, vol. 2937, pp. 239–251. Springer, Heidelberg (2004)

7. Bradley, A.R., Manna, Z., Sipma, H.B.: Termination analysis of integer linear loops. In: Abadi, M., de Alfaro, L. (eds.) CONCUR 2005. LNCS, vol. 3653, pp. 488–502. Springer, Heidelberg (2005)
8. Cousot, P.: Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming. In: Cousot, R. (ed.) VMCAI 2005. LNCS, vol. 3385, pp. 1–24. Springer, Heidelberg (2005)
9. Chen, Y., Xia, B., Yang, L., Zhan, N., Zhou, C.: Discovering non-linear ranking functions by solving semi-algebraic systems. In: Jones, C.B., Liu, Z., Woodcock, J. (eds.) ICTAC 2007. LNCS, vol. 4711, pp. 34–49. Springer, Heidelberg (2007)
10. Bradley, A.R., Manna, Z., Sipma, H.B.: Termination of polynomial programs. In: Cousot, R. (ed.) VMCAI 2005. LNCS, vol. 3385, pp. 113–129. Springer, Heidelberg (2005)
11. Babic, D., Hu, A.J., Rakamaric, Z., Cook, B.: Proving termination by divergence. In: SEFM 2007: Software Engineering and Formal Methods, London, England, UK, pp. 93–102. IEEE, Los Alamitos (2007)
12. Leue, S., Wei, W.: A region graph based approach to termination proofs. In: Hermanns, H., Palsberg, J. (eds.) TACAS 2006. LNCS, vol. 3920, pp. 318–333. Springer, Heidelberg (2006)
13. Wu, B., Bi, Z.: Termination of nested loop. In: ISCSCT 2008: International Symposium on Computer Science and Computational Technology, Shanghai, China, vol. 2, pp. 536–539. IEEE, Los Alamitos (2008)
14. Podelski, A., Rybalchenko, A.: Transition invariants. In: LICS 2004: Logic in Computer Science, Turku, Finland, pp. 32–41. IEEE, Los Alamitos (2004)
15. Tiwari, A.: Termination of linear programs. In: Alur, R., Peled, D.A. (eds.) CAV 2004. LNCS, vol. 3114, pp. 70–82. Springer, Heidelberg (2004)
16. Braverman, M.: Termination of integer linear programs. In: Ball, T., Jones, R.B. (eds.) CAV 2006. LNCS, vol. 4144, pp. 372–385. Springer, Heidelberg (2006)
17. Bi, Z., Shan, M., Wu, B.: Non-termination analysis of linear loop programs with conditionals. In: ASEA 2008: Advanced Software Engineering and Its Applications, Hainan Island, China, pp. 159–164. IEEE, Los Alamitos (2008)
18. Smart, D.R.: Fixed Piont Theorems. Cambridge University Press, Cambridge (1980)
19. Hoffman, K., Kunze, R.: Linear algebra, 2nd edn. Prentice-Hall, New Jersey (1971)
20. Xia, B., Zhang, Z.: Termination of linear programs with nonlinear constraints (2009), http://arxiv.org/abs/0904.3588v1

Development of Web Based Management Software for Safe Driving

Masaki Hayashi, Kazuhiro Hirata, Kazuaki Goshi, and Katsuya Matsunaga

Faculty of Information Science, Kyushu Sangyo University
2-3-1, Matsuka-dai, Higashi-Ku, Fukuoka, 813-8503, Japan
{k08djk03,k09gjk10}@ip.kyusan-u.ac.jp,
{goshi,matsnaga}@is.kyusan-u.ac.jp

Abstract. One of the goals of Intelligent Transport Systems (ITS) is to reduce traffic accidents and enhance safety. However, plenty of technologies for safe driving can not prevent traffic accidents, if a driver does not understand what safe driving is exactly. Thus, driver education is quite important even if ITSs spread. However, most educational methods for safe driving are subjective and lacking in concreteness. We have proposed safe driving theory based on a mechanism of collision and human cognitive characteristics. In this paper, we report an ASSIST, which stands for an Assistant System for Safe Driving by Informative Supervision and Training, and was created to prevent accidents based on our safe driving theory. The ASSIST uses sensors in a vehicle, computers, mobile phones and the Internet. We report development of web based management software for safe driving on the ASSIST.

Keywords: Intelligent Transport Systems (ITS), Safe Driving Theory, GPS, Internet, Summary.

1 Introduction

It is reported that more than a million souls are lost per year due to traffic accidents throughout the world. These losses have been a very serious problem to be solved.

To solve traffic problems, from the macro viewpoints, there are researches like traffic flow simulation or modeling [1-5]. On the other hand, we try to prevent traffic accidents from the educational viewpoints on Intelligent Transport Systems. One of the goals of Intelligent Transport Systems (ITS) is to reduce traffic accidents and enhance safety. However, plenty of technologies for safe driving cannot prevent traffic accidents, if a driver does not understand what safe driving is exactly. If the driver knew how to drive safely, warning systems or collision avoidance systems would be more effective in preventing traffic accidents. Thus, driver education is quite important even if ITS spread. However, most educational methods about safe driving are subjective and lacking in concreteness. We have proposed safe driving theory, which is called KM theory, based on a mechanism of collisions and human cognitive characteristics. Under the KM theory, we developed the driver support system. This time we have developed web based software for management of safe driving.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 497–509, 2010.

2 Computational Evaluation Method of Safe Driving

Traffic accidents occur when a vehicle's stopping distance is greater than the headway distance between it and other vehicles or obstacles as shown in Fig. 1.

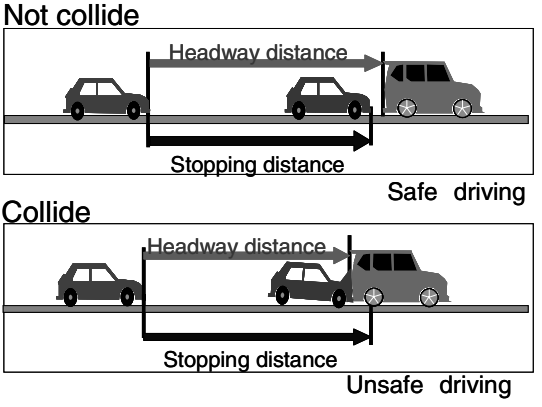


Fig. 1. Mechanism of collision

Stopping distance (right side of the inequality of (1)) is sometimes lengthened unexpectedly by a driver's sudden delay in cognition, while the headway distance (left side of the inequality of (1)) can be shortened by a driver's impulse to shorten traveling time. As a result, traffic accidents occur when the driver's headway distance becomes shorter than the stopping distance. Matsunaga found that a group of accident-prone drivers had a sudden lengthening of cognition and /or reaction time (braking time) [6]. Therefore, headway distance should be long enough to avoid a collision even if a sudden lengthening of stopping distance occurs.

$$Headway\ distance > Stopping\ distance \tag{1}$$

We introduced a collision prone index (CPI) shown in the equation (2) to estimate possibility of collision.

$$CPI = Stopping\ distance \,/\, Headway\ distance \tag{2}$$

Stopping distance can be calculated approximately from velocity as follows:

$$\begin{aligned} Stopping\ distance\ (m) &= rt \times v \times 1000 / 3600 \\ &+ (v \times 1000 / 3600)^2 \,/\, (2 \times g \times \mu) \end{aligned} \tag{3}$$

Where v (km/h) is the velocity of a vehicle, rt is braking time (here, rt=1.5s), and μ is coefficient of friction (here, μ=0.65).

We also introduced an unsafe time ratio shown in the equation (4) to evaluate degree of unsafety about specific time.

$$\textit{Unsafe time ratio} = \textit{unsafe time} / \textit{total time} \tag{4}$$

Where unsafe time is the sum total of time when CPI is greater than 1. To evaluate drive from start to return, the total time is the total travel time from start to return. To evaluate change through time, we divide the total traveling time from start to return every 10 minutes and each 10 minutes is used as total time.

We researched an educational method that could reduce hasty and speedy driving, which is one of the factors leading to a shorter headway distance. Some drivers usually drive their vehicles hastily in order to shorten traveling time. Researchers, however, have found that there were no meaningful differences in the traveling time when driving fast and when driving at ordinary speeds [7], because even if drivers increase velocity, stopping time at traffic signals also increases. Moreover, the former drivers suffered from stress and fatigue which requires those drivers to need to get some rest. In general, however, many drivers do not clearly understand the above matter. The research has also found that people who can understand the inefficiency of driving exceedingly fast via experience, learn to control it while driving.

The inefficiency of hasty driving is understood by comparing driving velocity with traveling velocity, because even if the driving velocity is high, the traveling velocity is not so high. In this paper, the term “driving time” is used to refer to time when velocity is higher than 0 and it does not include stop time at traffic signals. The term “traveling time” is used to refer to time that includes driving time and stop time at traffic signals. The term “parking time” is used to refer to time when the vehicle stay for a long time for delivery and collection or for a rest. The term “driving velocity” is used to refer to traveling distance divided by driving time. The term “traveling velocity” is used to refer to traveling distance divided by traveling time.

Crossroads are places where fatal traffic accidents happen most frequently. To avoid collisions at a crossroad without a traffic light, a driver should stop firmly and watch for a safe opportunity to continue driving. However, most drivers just slow down without completely stopping at the crossroad with a stopping enforcement while thinking their vehicles have stopped. If they do not stop firmly, it is easy to overlook vehicles or pedestrians. Moreover, even if a driver sees them, his/her vehicle still moves forward until it completely stops and the driver cannot help but have a collision in some situations. In recommended behavior at a crossroad near a building, the driver should stop at least twice as shown in Fig. 2. The driver should stop behind a particular stop line to avoid a collision with pedestrians or bicycles and the vehicle also needs to stop again in order to watch for oncoming vehicles that may be entering the crossroad.

We introduced an unsafe ratio about crossroads shown in the equation (5) to evaluate degree of unsafely about crossroad.

$$\textit{Unsafe ratio about crossroads} = \textit{number of crossroads without stopping} / \textit{total number of crossroads} \tag{5}$$

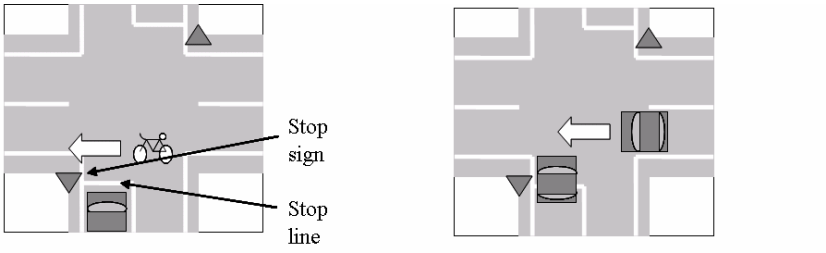


Fig. 2. Ideal behavior in an uncontrolled crossroad

3 ASSIST

3.1 Educational Topics

We are developing ASSIST which stands for an Assistant System for Safe Driving by Informative Supervision and Training based on our safe driving theory in section 2. The effectiveness of real time education of ASSIST was confirmed through experiments [8,9].

The ASSIST deals with three topics that are avoidance of rear end collision, avoidance of collision at an uncontrolled crossroad, and helping to learn inefficiency of hasty and speedy driving. The ASSIST can judge unsafe behavior on rear end collision by analyzing the CPI using a value of velocity, driver's reaction time, and a headway distance, and unsafe behavior at crossroads from velocity, position and database of positions where drivers should stop. The ASSIST can display maximum velocity and stop time related to inefficiency of hasty and speedy driving.

3.2 Method of Education

We designed the ASSIST that supports both the education after driving and the education in real time to teach them. In the education after driving, a computer keeps driver's behavior acquired by sensors in a vehicle, and a supervisor can educate drivers according to the behavior or the driver can manage his/her own behavior. In a conventional safety class, a supervisor can only say general contents about safe driving. However, in the education after driving by using the ASSIST, a supervisor can give advices to an individual driver according to the records of individual behavior. In the education in real time, the computer in the vehicle sends the information on driver's behavior acquired by sensors to a computer in a remote place and a supervisor can teach or warn the driver in real time according to the behavior that is shown visually on the screen of the computer in the remote place.

3.3 Hardware and Software

The ASSIST consists of an on-board system in a vehicle and a supervision system for the supervisor. In the on-board system, an embedded computer is connected with a GPS, a speed sensor, a laser distance measuring device and a video camera to obtain

the driver's behavior such as car location, velocity, headway distance and a front view image. A mobile phone is used for linkage between the on-board system and the supervision system. The supervision system has a computer that receives the data from the on-board system and shows information about a driver's behavior. The overview of ASSIST hardware is shown in Fig. 3.

The software for the on-board system records the driving behavior, judges of situation of unsafe driving, and transmits the data to the supervision system. A supervisor/safety manager can use a management software for ASSIST connection in real time education.

In education after driving, a supervision software can be used that has facilities of display of table, daily evaluation, search, and replay.

Both supervision softwares in real time and after driving can show recorded driving behavior by a digital map, graphs and a front view image.

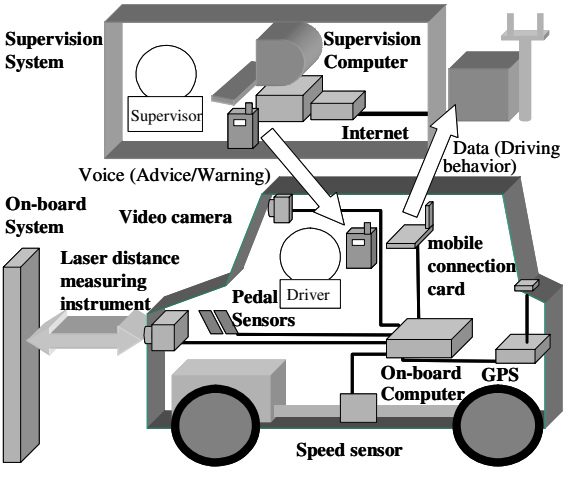


Fig. 3. Overview of the ASSIST hardware

4 Web Based Management Software

4.1 Design of the Web Based Management Software

In JAPAN, a transportation company of a certain amount of scale must set a safety manager. Until now, a safety manager could find only speedy driving by using a tachograph. However, traffic accidents occur even when velocity is low. The aim of this software is that the safety manager at a site of a transportation company can manage safe driving of drivers without using the special software. In order for the safety manager to use the software by himself easily, it should have web interface.

The software should show current information that includes CPI, velocity, headway distance, and position. The CPI, velocity, and headway distance are shown as numerical values and graphs. The position is shown on a digital map.

The software should also show evaluation about the driving behavior from start to now. The evaluation includes unsafe time ratio, traveling distance, total traveling time, driving time. When a vehicle returns to a base station of a transport company after collection and delivery, the software can show evaluation from start to return. This facility makes it possible for the safety manager to educate drivers just after returning to the base station. To realize this facility, we designed so that an on-board system might calculate total sums of unsafe time, velocity, total traveling time, and driving time for evaluation. Before developing this software, the safety manager must use a special software to evaluate driving behavior data and someone has to get the data from on-board system, while the vehicle is at the base station. Therefore the safety manager could not educate immediately after driver's returning and the education must be inefficient because the driver's memory fades as time passes.

4.2 Development of Web Based Management Software

The web based management software consists of a recording program, an evaluation program, a transmitting program, an ASSIST server program and a web interface. Fig.4 shows the flow of information on the Web based management software. We use C language to develop the recording program, the evaluation program, the transmitting program and the ASSIST server program and use HTML, PHP, and JavaScript language to develop the web interface.

The recording program of on-board computer saves a front view image from a camera and numerical data that includes velocity, headway distance, car's ID, driver's ID, system time, latitude, longitude from sensors. The recording program sends numerical data to evaluation program through UDP socket and saves a front view image to external memory unit or a solid state disk (SSD) that we use.

The evaluation program calculates adding up of velocity, driving time, stopping time, parking time and unsafe time every 10 minutes as summary. The evaluation program sends the summary data to the transmitting program through UDP socket after calculation.

The transmitting program sends live data, summary data, and unsafe data to the server of ASSIST through TCP socket on mobile network. The live data consists of time, car's ID, driver's ID, latitude, longitude, velocity, headway distance, direction and a front view image. The data of velocity and headway distance and direction is data for 20 seconds to draw graphs. The summary data includes sequence of time index, sum total of velocity, sum total of stopping time, sum total of parking time and sum total of unsafe time for every 10 minutes. The unsafe data includes CPI and front view images when longest unsafe condition happened.

The ASSIST server program saves live data, summary data, and unsafe data to the server's hard disk. A text file named data.txt and as a jpeg image file named img.jpg are saved as the live data. A text file named summary.txt is saved as the summary data. A text file named longest.txt and image files are saved as the unsafe data.

The web interface shows information based on the files of data.txt, img.jpg, summary.txt, longest.txt, and image files for unsafe data by using a web server and a web browser.

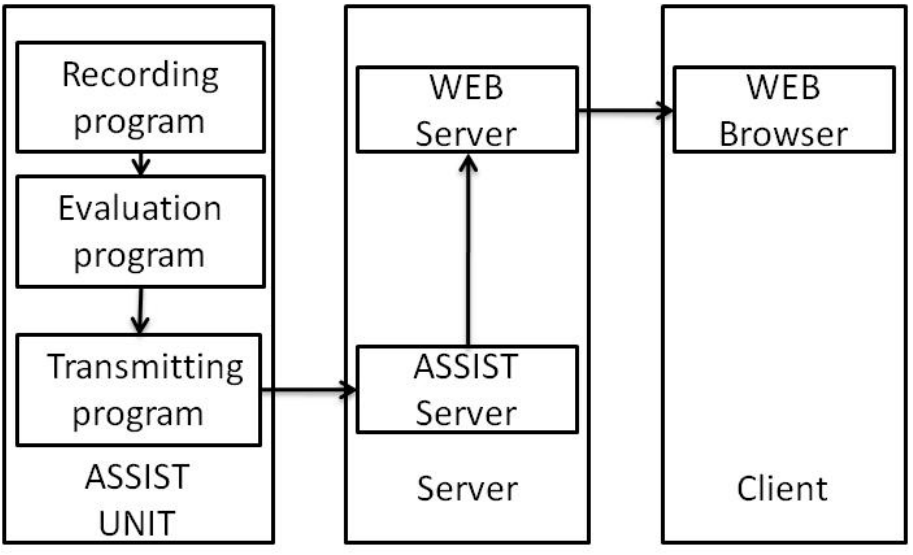


Fig. 4. Structure of the ASSIST

4.3 Detail of the Evaluation Program

As mentioned in section 4.1, in order for the safety manager to educate drivers based on evaluation of safe driving just after driver's returning to the base station, we developed the evaluation program in a vehicle to calculate total sums of unsafe time, velocity, total traveling time, and driving time. Until now the calculation was done after getting driving behavior data from the vehicle and it took time until the evaluation is available. If the communication infrastructure has sufficient capability to send all driving behavior data, the evaluation can be done by a computer for safe driving manager in a remote place. However, because we use the mobile data connection service that speed is only 17 kbps and the connection is often closed by radio wave condition, it is impossible to send all data. Thus we decided to evaluate by the computer in the vehicle and send the result of evaluation to a computer for the safety manager. The evaluation program calculates degree of safety based on our computational evaluation method in the vehicle and sends it to the ASSIST server at remote place every 10 minutes.

When the on-board system starts by vehicle's engine starting, the recording program makes a new text file for numerical value of driving behavior and appends current data every second. Thus, if the driver starts and stops the vehicle's engine several time from start to return, several text files are made. The evaluation program calculates total sum from several text files of past driving behavior data and current driving behavior data from the recording program as shown in Fig. 5.

Another simple method to calculate against several files is that the evaluation program makes an individual file of total sum against every file of driving behavior and joins the individual files. However the evaluation program has to update files of total sum every second, because the on-board system is always suddenly turned off

without shutdown process by engine's stop. This simple method makes calculating time shorten, however, we did not chose this method, because frequent updates cause troubles in the external memory unit by the write limit of the solid state disk.

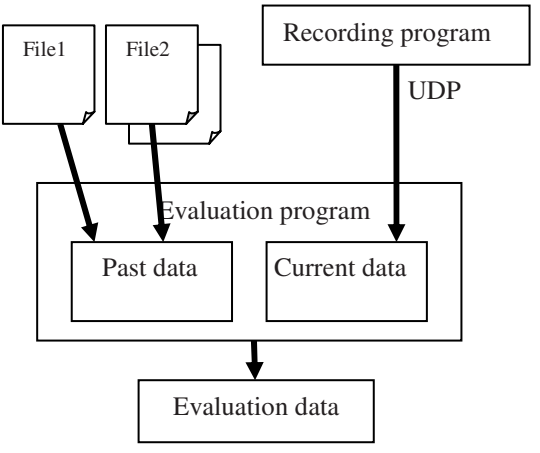


Fig. 5. Evaluation program

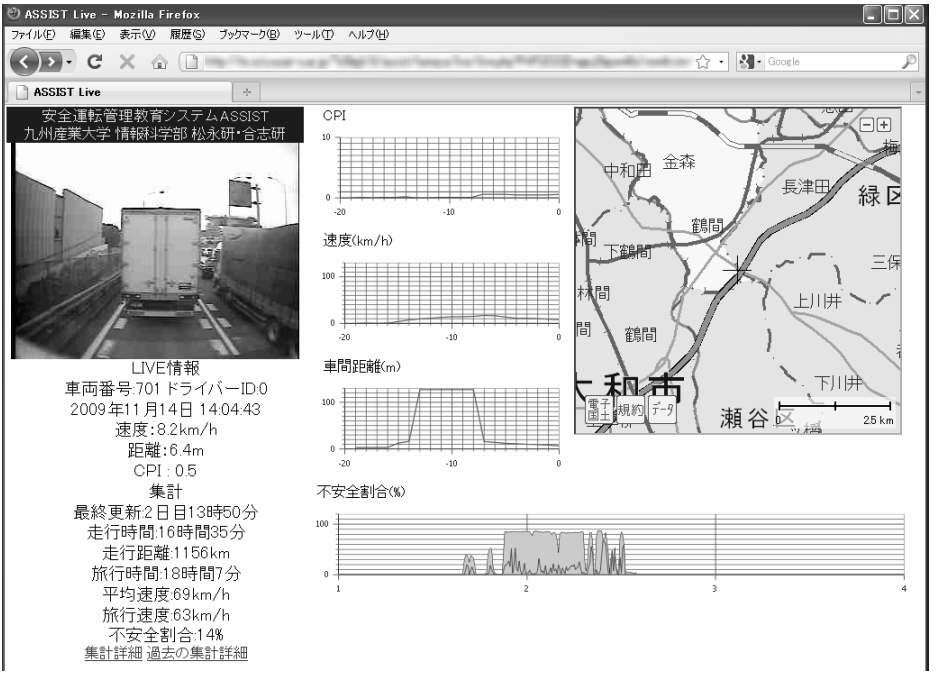


Fig. 6. An example of screen of Web-based Supervision Software

4.4 Detail of the Web Interface

We developed the web interface for safety manager to check driving behavior. We use PHP for user authentication and JavaScript with Dojo Toolkit [10] for updating data and drawing graphs. We also use Denshi Kokudo digital map [11] to show current position. And we use web API of reverse geocoding service [12] to show a place name of current position. The interface automatically updates live data every 10 seconds and the summary data every 10 minutes by using AJAX.

A screen of top page of the web interface is shown in Fig. 6. On the left side of the screen, there are a front view image, information of live data, and the information of the summary. The information of live data includes latest update time of the information, car's ID, velocity, headway distance, and CPI. And the summary data includes latest update time of the information, traveling distance, driving time, traveling time and unsafe time ratio. On the center of the screen, there are graphs of CPI, velocity, headway distance, and unsafe time ratio (red line) with average of velocity (blue line). On the right side of the screen, there is the digital map around current position. The top page also includes link of detail of the current summary and link of list of the past summaries.

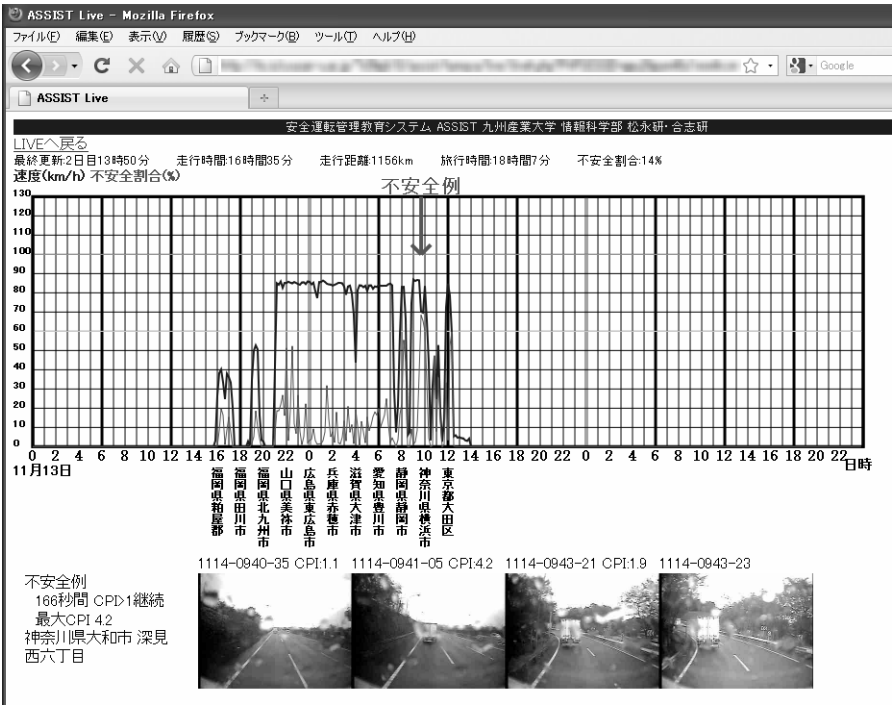


Fig. 7. An example of screen of the page of detailed current summary

A screen of the page of detail summary is shown in Fig. 7. On the top part of the screen, there are traveling distance, driving time, traveling time, average velocity, traveling velocity and unsafe time ratio. On the middle part of the screen, there is a graph of unsafe time ratio with average velocity. We put place names in addition to time and date on the x-axis. On the bottom part of the screen, there is the unsafe data. It includes four images, CPI and the place name when the unsafe events happened.

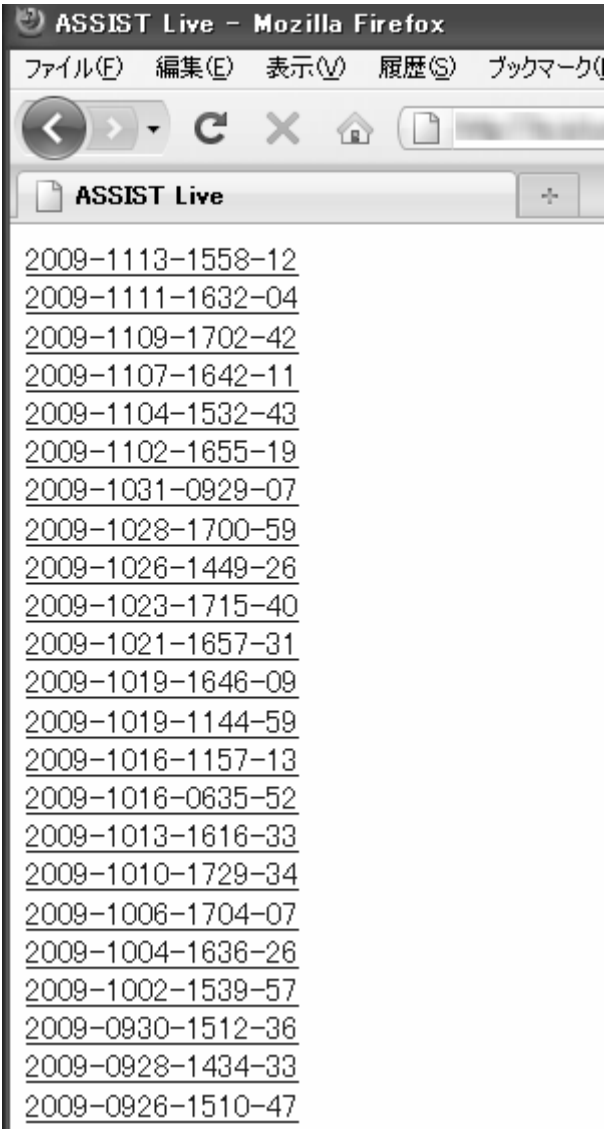


Fig. 8. An example of screen of the page of past summaries list

A screen of the page of past summaries list is shown in Fig. 8. It shows links to past detailed summary pages. A page that the link represents is similar to the page of detailed current summary.

5 Preliminarily Evaluation of Web Based Management Software

We told the URI of the web interface, account name and password to a safety manager of a transport company in which we had asked to put the on-board system of ASSIST on a long-haul truck. After using it several times, he expressed the comment that it was good to get information immediately just after the truck's return and to be able to know unsafe situation. In Fig.9, the unsafe ratio was 10% and that means appreciably safe driving. Meanwhile, in Fig.10, the unsafe ratio was about 30% and that means rather dangerous driving. We are going to talk with a safety manager and to perform more detailed evaluation of the software for further improvement.

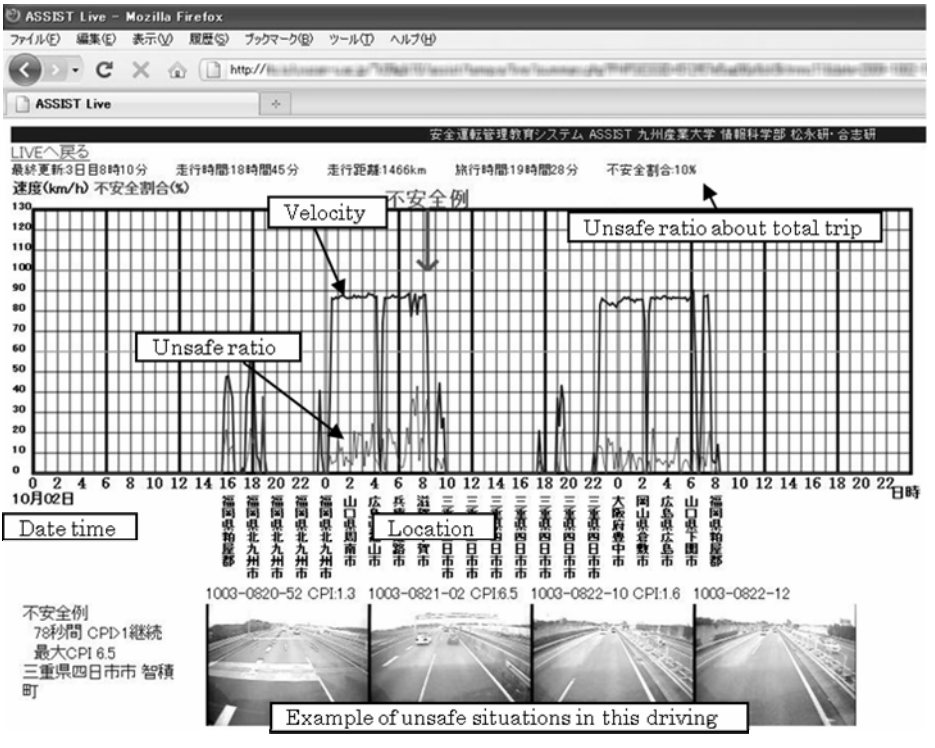


Fig. 9. An example of screen of the page of unsafe ratio is low

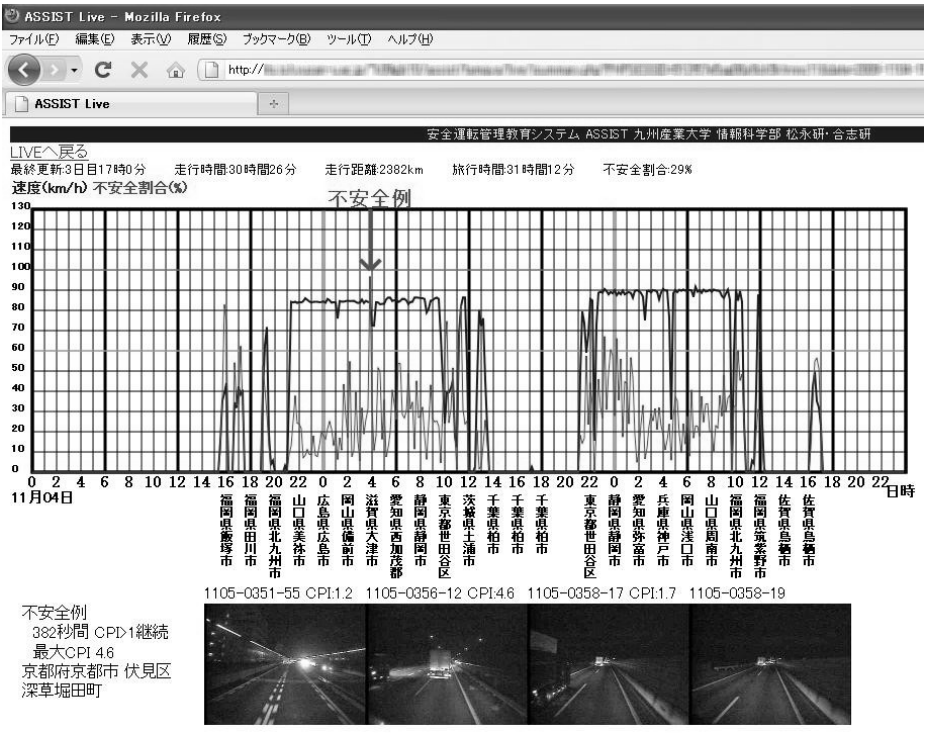


Fig. 10. An example of screen of the page of unsafe ratio is high

6 Conclusion and Future Studies

We have developed the web based management software for a safety manager to grasp the current situation and the evaluation from start to now. It is possible for the safety manager to educate a driver immediately just after the driver returns.

We will improve the software to show more individual unsafe information. After that we will evaluate the usability and educational effect of the software.

References

1. Li, Z.P., Liu, F.: Cellular Automaton Based Simulation for Signalized Street. International Journal of Engineering and Interdisciplinary Mathematics 1(1), 11–22 (2009)
2. Li, M., Zhao, W.: Representation of a Stochastic Traffic Bound. IEEE Transactions on Parallel and Distributed Systems (2009)
3. Cremer, M., Ludwig, J.: A fast simulation model for traffic flow on the basis of Boolean operations. Mathematics and Computers in Simulation 28(4), 297–303 (1986)
4. Gipps, P.G.: Multsim: a model for simulating vehicular traffic on multi-lane arterial roads. Mathematics and Computers in Simulation 28(4), 291–295 (1986)
5. Liatsis, P., Tawfik, H.M.: Two-dimensional road shape optimisation using genetic algorithms. Mathematics and Computers in Simulation 51(1-2), 19–31 (1999)

6. Matsunaga, K., Kito, T., Kitamura, F., Shidoji, K., Yanagida, T.: Reaction Time Variability and Type of Personality of Accident-Prone Drivers. In: Proceedings of the 22nd International Congress of Applied Psychology, Kyoto, p. 323 (1990, 1992)
7. Cohen, J., Preston, B.: Causes and Prevention of Road Accidents, p. 65. Faber and Faber Limited, London (1968)
8. Goshi, K., Matsunaga, K., Kuroki, D., Shidoji, K., Matsuki, Y.: Educational Intelligent Transport System ASSIST. In: Proceedings of the Fourth IASTED International Conference Computers and Advanced Technology in Education, Banff, pp. 150–154 (2001)
9. Watanabe, S., Matsunaga, K., Goshi, K., Shidoji, K., Matsuki, Y.: Development of An Intelligent Driving Support System for Commercial Vehicle Drivers. In: Proceedings of the 11th World Congress on ITS, Nagoya, CD-ROM #35 (2004)
10. The Dojo Toolkit, `http://www.dojotoolkit.org/`
11. Denshi Kokudo digital map, `http://portal.cyberjapan.jp/index.html`
12. Reverse geocoding service, `http://www.finds.jp/wsdocs/rgeocode/index.html`

A Study on Comparative Analysis of the Information Security Management Systems*

Heasuk Jo, Seungjoo Kim, and Dongho Won**

Information Security Group,
School of Information and Communication Engineering, Sungkyunkwan University,
300 Chunchun-dong, Suwon 440-746, Republic of Korea
{hsjo,skim,dhwon}@security.re.kr
http://www.security.re.kr

Abstract. Due to the advance of mobile network, E-commerce, Open Networks, and Internet Banking, Information Security Management System (ISMS) is used to manage information of their customer and themselves by a government or a business organization . The best known ISMSs are BS7799/ISO17799, Common Criteria, which are international standard. And some nations use their own ISMS, e.g., DITSCAP of USA, IT Baseline Protection Manual of Germany, ISMS of Japan. The paper explains the existed ISMSs and presents a comparative analysis on difference among ISMSs. The discussion deals with different aspects of types of the ISMSs: analysis on the present condition of the ISMSs, certification structure, and certification evaluation process. The study contribute so that a government or a business organization is able to refer to improve information security level of the organizations. The case study can also provide a business organization with an easy method for building ISMS.

Keywords: Information Security Management System(ISMS), Information Security Evaluation, Information Security Check, Information Security Evaluation Process.

1 Introduction

In the present day world, information security is an important issue in information intensive businesses. A fate of organization is decided, according as how many have information technology and how safely protect information. For effective management of information security in organization, Information Security Management Systems(ISMSs) are developed. ISMS manages and operates continuously information security system, in terms of technology, management, and

* This research was supported by the Ministry of Knowledge Economy, Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2009-(C1090-0902-0016)).

** Corresponding author.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 510–519, 2010.

hardware, for the aim of the information security that is to achieve confidentiality, integrity, and availability.

In current, there are various kind of ISMSs such as BS7799 of EU, Common Criteria, DITSCAP of USA, IT baseline protection Manual of Germany, and etc. BS7799, at the beginning, was developed for only own country, but in 2005, it was adopted as international standard, which was named to ISO/IEC 2700x[9]. Japan had developed own ISMS for itself. Later, Japan adopted several things of international standard(BS7799-2:2002) in 2002 and made JIS X 5080:2002[5]. DIACAP(Department of Defense DoD Information Assurance Certification and Accreditation Process) has replaced previous standard, DITSCAP. As stated above, various ISMSs are revised and developed.

In this paper, we explain a definition, a scope, a history, a structure, and etc. of the international standard and each national standard of ISMSs. And we discuss a comparative analysis of a difference of ISMSs which include management process, control specification, certification evaluation method, and post management. This paper can help a government or a business organization apply proper ISMS to their business and improve information security level of the organization. A study, moreover, can be used to develop new ISMS for business.

The remainder of this paper is organized as follows. Section 2 explains trend of the ISMSs. Section 3 provides the comparative analysis of the ISMSs. Finally, section 4 concludes the paper.

2 Trend of ISMSs

This section contains the trend of ISMSs for information security in the organization. The systems help organization for protection and maintenance of information assets(hardware, software, data, document, network, and etc.).

2.1 Common Criteria

The Common Criteria (CC)[1,2,3,4] is an internationally approved set of security standards(ISO/IEC15408) which provides a clear and reliable evaluation of the security capabilities of Information Technology(IT) products. The CC was developed by the governments of Canada, France, Germany, Japan, the Netherlands, Spain, the UK, and the U.S. It was published in 1993 and current version 3.1 of the CC has been continuously developed and revised. This history is as follows:

- 1998 : CC 2.0
- 1999 : CC 2.1 (ISO15408:1999)
- 2004 : CC 2.2 (ISO FCD)
- 2005 : CC 3.0 (Draft)
- 2005 : CC 2.3 (ISO 15408:2005)
- 2006 : CC 3.1 (Release 1)
- 2007 : CC 3.1 (Release 2)

Objective of the CC is providing a basis for evaluation of security properties of IT products, a means to mutual recognition for IT security evaluation, and an offer of standard category of security function and security assurance requirement. The CC consists of the followings 3 parts[4]:

- *Part* 1 *Introduction and general model*:
- *Part* 2 *Security functional components*: It describes a set of security functional components(families and classes) that provide standard templates to base function requirements for TOEs(Target Of Evaluation) which means a set of software and/or hardware possible accompanied by guidance.
- *Part* 3 *Security assurance components*: It describes a set of assurance components that provide standard templates to base assurance requirements for TOEs. It defines evaluation criteria for PPs(Protection Profile) and STs(Security Target) and introduces assurance packages(Evaluation Assurance Levels, EALs)

Target audience of the CC is consumers, developers, and evaluators who can use 3 parts of the CC. Road map to the CC is as follows, Table 1.

Table 1. Road Map to the Common Criteria[1]

	Consumers	**Developers**	**Evaluators**
Part 1	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference purposes. Development of security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for a TOE.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Use for reference when interpreting statements of functional requirements.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use for reference when interpreting statements of assurance requirements.

2.2 BS7799

BS7799 was published by the British Standards Institute(BSI) in 1995. It consists of two parts. The first part, "Code of Practice for Information Security Management(BS7799 Part 1[7])", is published in 1995, and written by the United Kingdom Government's Department of Trade and Industry. It is a comprehensive set of information security controls. It was adopted as International standard

by the Joint Technical Committee ISO/IEC JTC1(Information technology)/SC 27(IT Security techniques). ISO/IEC 17799:2000[7,8,9] was prepared by the committee and published in 2000. ISO/IEC 17799:2005 was revised in 2005 and was renumbered as ISO/IEC 27002 in 2007. ISO/IEC 27002 is a document written for information security management controls. ISO/IEC 27002 consists of 39 control objectives of the 11 subjects to protect information assets against threats. Each objective has several components. The standard contains the following eleven main subjects:

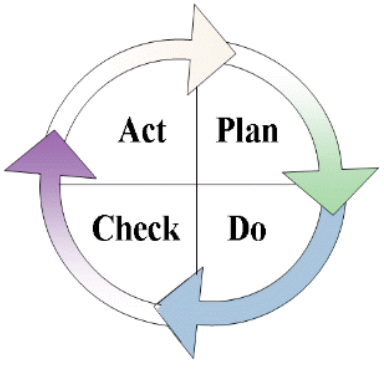


Fig. 1. Plan-Do-Check-Act model

- *Security policy*: Information security policy, Other security policy
- *Organization of information security*: Internal organization, External parties
- *Asset management*: Responsibility for assets, Information classification
- *Humanresourcessecurity*: Prior to employment, During employment, Terminating or change of employment
- *Physical and environmental security*: Secure areas, Equipment security
- *Communications and operations management*: Operational procedures and responsibilities, Third-party service delivery management, System planning and acceptance, protection against malicious and mobile code, back-up, Network security management, Media handling, Exchange of information, Electronic commerce services, Monitoring
- *Access control*: Business requirements for access control, User access management, User responsibilities, Network access control, Operating system access control, Application and information access control, Mobile computing and teleworking
- *Information systems acquisition, development and maintenance*: Security requirements of information systems, Correct processing in applications, Cryptographic controls, Security of system files, Security development and support processes, Technical vulnerability management 10. Information

security incident management - Reporting information security events and weaknesses, Management of information security incidents and improvements
- *Information security incident management*: Reproting in information security events and weaknesses, Management of information security incidents and improvements
- *Business continuity management*: Information security aspects of business continuity management
- *Compliance*: Compliance with legal requirements, Compliance with organizational security policies, tech standards, Information systems audit considerations

The second, BS7799 part 2,"Information Security Management Systems Specification with guidance for use", was published by BSI in 1999. BS7799-2(BS7799 part 2) focused on how to implement the information security management structure. It referenced the control information identified by ISO17799. BS7799-2 introduced the Plan-Do-Check-Act(PDCA) in 2002, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005[8]. The following diagram illustrates the PDCA model, Fig.1:

- *Plan*: Establish ISMS, Identify assets
- *Do*: Implement and operate the ISMS
- *Check*: Monitor and review the ISMS
- *Act*: Maintain and improve the ISMS

Over 4,700 organizations worldwide have already been certified compliant with ISO/IEC 27001 or equivalent national variants, Fig.2:

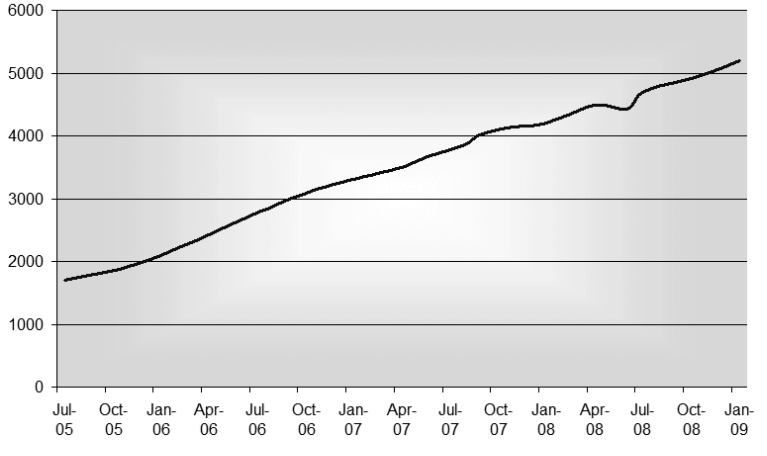


Fig. 2. Number of ISO/IEC 27001(or equivalent Certifications)[9]

2.3 IT Baseline Protection Manual

IT baseline protection manual(ITBPM)[10,11] is focused on methodology of a IT security management for a IT system by Germany Federal office(known as BSI, Bundesamt Fur Sicherheit in der Informationstechnik). The ITBPM was published the first version in 1994 and has been further developed since then. It provides both a methodology for setting up a management system for information security and a comprehensive basis for monitoring the existing IT security level and implementing appropriate IT security. ITBPM model divides five tiers according to a IT security aspects of a set of IT assets. These tiers are follows[10]:

- *Tier* 1 : *Universally applicable aspects* This covers all the general IT security aspects which apply equally to all or large numbers of the IT assets, particularly any universally applicable concepts and the procedures derived therefrom. Typical Tier 1 modules include IT Security Management, Organization, Personnel, Contingency Planning, Data Backup Policy, Data Privacy Protection, Concept of computer virus protection, Cryto-concept, Handling of security incidents, Hard and Software-Management, and Outsourcing.
- *Tier* 2 : *Infrastructure* This is concerned with architectural and structural factors, in which aspects of the infrastructural security are brought together. This concerns especially the Buildings, Cabling, Office, Server room, Data media archives, Technical infrastructure room, protective cabinets, Working place at home, and Computer centers.
- *Tier* 3 : *IT systems* This concerns the individual IT systems in the set of IT assets which may be grouped together. The IT security aspects considered here relate not only to clients but also to servers and stand-alone systems. Trier 3 modules include DOS-PC, Unix-System, Laptop PC, Windows NT PC, Internet PC, Server-supported Network, Unix-Server, Router and Switches, Telecommunication System, Fax machine, and etc.
- *Tier* 4 : *Network* This concerns the networking aspects of the IT systems, which refer to the network connections and communications rather than to particular IT systems. The modules which are relevant here include, for example, Heterogeneous Networks, Network and System Management , Modem, Firewall, Remote Access, and LAN integration of a IT system via ISDN.
- *Tier* 5 : *IT applications* This is concerned with the actual IT applications which are used on the IT assets. In this tier, the modules used for modelling purposes could include Exchange of Data Media, E-Mail, WWW Server, Lotus Notes, Internet Information Server, Apache Webserver, Exchange/Outlook 2000, Fax Server, Databases, and Novelle Directory.

2.4 ISMS in Japan

In 2001, ISMS certification criteria(Ver.0.8)[5] of Japan was firstly developed based on both the BS7799-2 and ISO/IEC 17799, since then it has been further developed. After, ISO/IEC 27001:2005 of international standard for information

security management systems was issued in October 2005, ISMS certification criteria(Ver.2.0) were replaced with JIS Q 27001. JIS Q 27001 applies Plan-Do-Check-Act(PDCA) model as BS7799. The implement of the ISMS is divided into three phases[5,6]:

- *Phase* 1(STEP1-STEP2): The scope of the ISMS should be established considering assets and technology of the organization. An organization defines an policy for the method of risk management and operation environment.
- *Phase* 2(STEP3-STEP7): An organization evaluates existed threat in organization then establishes alternative plan for relief of threats.
- *Phase* 3(STEP8-STEP10): After an organization certificate to mitigate the identified threats to Phase 2, if it safety reach information security level of an organization, obtain management authorization to implement the ISMS.

The following Fig.3 shows three phases.

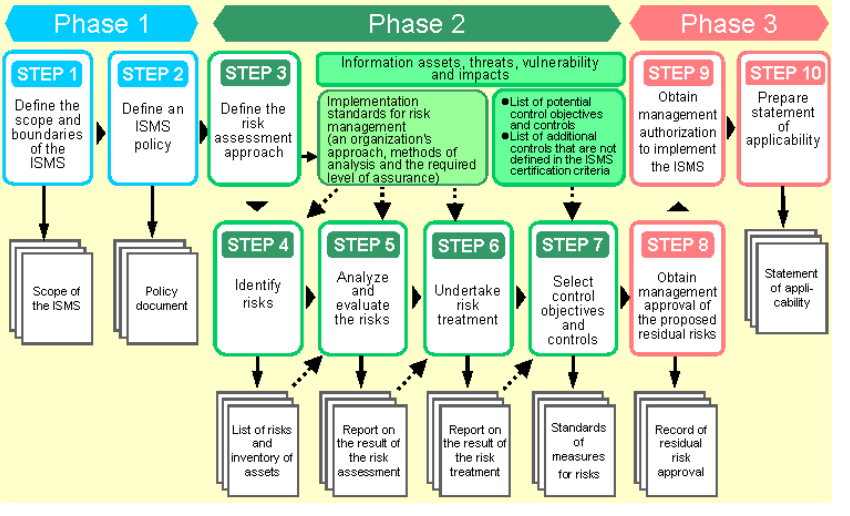


Fig. 3. Three phases for establishment of the ISMS[5]

2.5 DITSCAP

Defense Information Assurance Certification and Accreditation Process(DITSCAP) is a standard process defined by the United States Department of Defense(DoD) for managing risk. It establishes a set of activities, general tasks and a management structure to certify and accredit for the Defense Information Infrastructure(DII) and the Information Assurance[12,13]. The main objective of DITSCAP is adaptable any system mission, computing environment, and architecture. It has flexibility in the whole life-cycle to apply information security evaluation and accreditation. The DITSCAP process consists of the followings four phases:

- *Phase* 1 *Definition* The Definition phase plans activities of certification and accreditation(C&A) and gains the necessary information to understand information system. It defines system mission, environment, architecture, and levels of effort for C&A and identify the threat. The output of phase 1 is documented in the System Security Authorization Agreement(SSAA). SSAA is *"used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security"* [12,14].
- *Phase* 2 *Verification* The process of phase 2 verifies the evolving system's compliance with the information security requirement during system development and modification in the life-cycle of the information system. A verification phase starts with a review of the SSAA which shall be documented and updated the overall modification or development factor since the Definition phase 1. It must be known that any changes of system through the updated SSAA to the DAA(Designated Approving Authority), the CA(Certification Authority), the program manager, and the user representative.
- *Phase* 3 *Validation* The phase 3 validates fully integrated system compliance with the security requirements. The SSAA must be firstly reviewed to ensure that its requirements and agreements still apply as Phase 2. The SSAA includes details of the current state of the system. It must be submitted that required changes of system through the updated SSAA to the DAA, the CA, the program manager, and the user representative for the approval and the execution of revised agreement.
- *Phase* 4 *PostAccreditation* Finally, Post Accreditation phase includes activities to operate and manage the system for maintenance of an acceptable level of risk. The phase is continually applied from installation of the integrated system to being disused in life-cycle.

3 Comparison and Analysis of the ISMSs

This section analyzes and compares structure and certification evaluation process of the ISMSs. The CC is consisted of 3 parts which is divided into 11 security functional requirements, and 8 assurance requirements in detail. The BS7799 is consisted of 11 security domains, 139 control objectives, and 133 security controls. The ITPMG is consisted of 8 steps and 62 modules on technical and non-technical aspects of IT security. The DITSCAP is consisted of 4 management phases, 16 control objectives, and 39 service units.

Although BS7799 lays emphasis on the management of information security than the DITSCAP, it do not have a way of pre-evaluation about assets and not enough in terms of technology of information security. CC, ITPMG, and DITSCAP lay emphasis on terms of technology of information security, however these are insufficient in terms of the management of information security. In the case of the ISMS in Japan, it has 3 management phases consisted of 10 steps. This system is similar with BS7799, therefore we omits comparison and analysis. The Table 2 illustrates the certification structure comparison of the ISMSs.

Table 2. The certification structure comparison of the ISMSs

	CC	BS7799	ITPMG	DITSCAP
Basic Structure	□3 Parts □11 Security Functional Requirements □8 Assurance Requirements	□6 Management Phases □11 Security Domains □139 Control Objectives □133 Security Controls	□8 Steps □62 Modules	□4 Management Phases □16 Control Objectives □39 Service Units
Management Process	1. PP/ST introduction 2. Conformance claims 3. Security problem definition 4. Security objectives 5. Extended components definition 6. Security requirements 7.TOE summary specification	1. Define policy 2. Define scope 3. Assess risk 4. Manage risk 5. Select controls to be implemented and applied 6. Prepare a statement of applicability	1. Assess protection requirements 2. Security concept 3. Check basic security level 4. Define changeable checklists 5. Check reasonable level of protection 6. Identify implementation 7. Self-certification	1. Definition 2. Verification 3. Validation 4. Accreditation
Difference of Process	□Emphasis on technology of information security	□Emphasis on technology of information security	□Emphasis on technology of information security	□Emphasis on management of information security
Specification Control Point	□Provide common set of requirements for the security functionality of IT products	□Provide best code of practice for information security management	□Provide correspondence method with IT infrastructure and modules	□Protect information system and defense information infrastructure
Certification Evaluation Method	□Follow each certification evaluation procedure	□Use the PDAC model cycle	□The permitted auditor by BSI certify	□Follow C&A process
Post management	□Until the product life finishes	□once by six months	□Until the system life finishes	□When the system changes

4 Conclusion

ISMSs are developed for a government or a organization that should protect their information assets and intercept any existing risks for secure information management of their customer and themselves.

ISMS manages and operates continuously information security system, in terms of technology, management, and hardware through life-cycle to apply information security evaluation and accreditation. In current, ISMS exists variety systems which are CC, BS7799, IT baseline protection manual, ISMS in Japan, DITSCAP, and etc. In this paper, we was descriptive of various ISMSs which include history, scope, development organization, process structure, and etc. And we made an analysis of different the ISMSs: analysis the present condition , basic structure, certification evaluation process, management process, post management. The study provide that a government or a business organization in need of information security may be able to refer to improve information security level of the organizations. The case study can be also contributed to build the ISMS in a business organization.

References

1. International Standard ISO/IEC 15408, Common Methodology for Information Technology Security Evaluation,Version 3.1, 2006.10
2. International Standard ISO/IEC 15408, Common Criteria for Information Technology Security Envluation, Part1,Version 3.1, 2006.10
3. International Standard ISO/IEC 15408, Common Criteria for Information Technology Security Envluation, Part2,Version 3.1, 2006.10
4. International Standard ISO/IEC 15408, Common Criteria for Information Technology Security Envluation, Part2,Version 3.1, 2006.10
5. Japan Information processing development corporation, JIS Q 27001 (ISO/IEC 27001:2005) Information security management sytem conformity assessment scheme (2006)
6. JIPDEC, http://www.isms.jipdec.jp/en/index.html
7. BSI, BS7799 Part 2: Code of Practice for Information Security Management, British Standards Institute (1999)
8. ISO, International Standards ISO/IEC 27001, Information technology Security techniques-Information security management systems-requirements (2005)
9. http://www.iso27001security.com/html/27000.html
10. IT Baseline Protection Manual (2004)
11. IT Baseline protection Manual Layer model, http://www.bsi.bund.de/english/gshb/manual/schichtenmodell.htm
12. DoD 5810.1-M: DITSCAP Applicatio Manual (2001)
13. Valletta, A.M.: DoD Instruction (1997)
14. DoD Information Assurance, http://www.ati4it.com/DOD

Beacon-Based Cooperative Forwarding Scheme for Safety-Related Inter-Vehicle Communications

Songnan Bai, Zequn Huang, and Jaeil Jung*

Department of Electronic and Computer Engineering
Hanyang University, Seoul, Korea
{songnam,zequn,jijung}@hanyang.ac.kr

Abstract. Most safety-related applications targeting Inter-Vehicle Communications systems (IVC) rely on multi-hop broadcasts to disseminate safety-related information to all surrounding vehicles. However, these conventional broadcast schemes suffer from the so-called "broadcast storm" problem, a scenario in which contention and collisions happens a lot due to an excessive number of broadcast packets. In this paper, we propose a novel solution, referred to as the Beacon-based Cooperative Forwarding (BCF) scheme for fast and reliable propagation of safety message within a critical area. With the aid of periodic beacons, the proposed scheme specifies multiple appropriate forwarder candidates to broadcast the alert message before detecting a danger. Moreover, a cooperative forwarding scheme is also proposed to guarantee high reachability and to delay constraints. After realistic simulations, the BCF scheme demonstrated better performance than other contention-based schemes by reducing the end-to-end delay and message rebroadcasting ratio by over 30% while maintaining a high message reception rate.

1 Introduction

Inter-Vehicle Communications (IVC) are now considered to be suitable for enhancing road safety and efficiency in vehicular environment. Especially after the allocation of the 75MHZ spectrum at the 5.9GHZ frequency band for Intelligent Transport Systems (ITS), several national and international projects, e.g., Vehicle Safety Communication Consortium (VSCC) in the USA [1], Advanced Driver Assistance Systems in Europe (ADASE) [2] are initially intended for active safety applications that aim to avoid or decrease the road accidents.

In order to develop optimal solutions for IVC, the communication environments and characteristics of safety-related applications should be considered. First, IVC systems consist of high mobility vehicles moving in the same or opposite directions along the road. Second, in real scenarios, nodes can experience signal strength attenuation due to reflection and distortion between radio waves and the environment [3]. However, most previous researches just consider the simplistic assumptions that are quite opposite to real scenarios. Moreover, safety

* Corresponding author.

D. Taniar et al. (Eds.): ICCSA 2010, Part IV, LNCS 6019, pp. 520–534, 2010.

applications are characterized by strong reliability and delay requirements. Due to the applications' safety requirement, it is envisioned that multi-hop broadcasting will be the most common strategy to propagate safety-related information to all surrounding vehicles within a certain geographic area [4-5].

However, the conventional broadcast schemes for IVC such as pure flooding has drawbacks where simultaneous broadcasting among neighbor nodes can lead to frequent contention and collisions due to excessive number of broadcast packets. This issue is also referred to as the "broadcast storm problem", which can cause an unbearably large delay and packet loss in IVCs. Additionally, due to the shared wireless medium, the CSMA/CA MAC based broadcast is especially sensitive to hidden terminal problem and no-MAC level recovery mechanisms are provided for the transmission failure [6]. Therefore, it is important to design a reliable and efficient Vehicle-to-Vehicle (V2V) broadcasting protocols to support safety applications.

In this paper, we first pay attention to the random characteristic of realistic radio propagation channel, which is often omitted in wireless research. Motivated by the analysis results, we propose a novel broadcasting scheme referred to as Beacon-based Cooperative Forwarding (BCF) scheme, which specifies multiple reliable forwarder candidates to broadcast the alert message before detecting a danger. To mitigate contention, all the forwarder candidates are assigned with different forwarding delay according to their relative distance. Based on previous studies, we identify the need of a mechanism to prevent random packet loss due to hidden terminal problem, radio attenuation and heavy link load in dense traffic situations: thus, we propose a cooperative forwarding strategy to help forwarding when all the specified forwarder candidates fail to transmit the message.

The remainder of the paper is organized as follows. First, we review some related researches and the necessary background in IVCs. Then, we present the detailed mechanism of BCF protocol operation in section 3. In section 4, we describe the highway scenarios, simulation parameters and the performance analysis. Finally, the conclusions and future works are descripted in section 5.

2 Related Works

2.1 Routing Protocols

Before the protocols description, we present the studies and approaches related to our work. Most broadcast protocol targeting at IVCs can be divided into two categories: beacon-less and beacon-based approaches [7].

Most beacon-less approaches used in IVCs are also a type of contention-based scheme, that allows each node to calculate its own rebroadcast probability or forwarding delay time according to its position information. Weighted-p scheme [8] assigns higher rebroadcasting probability to nodes that are located farther away from the sending node. In Sloted-1 [8], the broadcast coverage is spatially divided into several regions and a shorter waiting time is assigned to the nodes located in the farthest region. The Delayed Broadcasting Protocol (DDB) [9]

calculates the rebroadcast waiting time by considering the cover additional area (AC) when receiving a duplicated packet each time.

These contention-based schemes can mitigate contention effectively by allowing nodes rebroadcasting with different priorities based on the relative distance between itself and the sender. However, the performance of these schemes are highly sensitive to the chosen threshold (e.g., waiting period in Weighted-p, number of slots in Slotted-1 and maximum waiting time in DDB), which are hard to predict and especially cannot be changed adaptively according to various traffic density.

The beacon-based schemes have the advantage of acquiring neighbor relationship with the aid of a periodic hello message. In [10], the node rebroadcast probability is dynamically determined depending on the estimation of local vehicle density information. And in [11], each node continuously monitors its local connectivity situation to determine the optimized broadcasting suppression algorithms. However, the scheme relies heavily on accurately detecting the local connectivity information and this neighbor information may be out-of-date due to high mobility.

Furthermore, all those schemes use an idealistic radio propagation model (e.g., Two-Ray ground) and a simple error model to evaluate the performance. Unfortunately, these ideal assumptions are quite unrealistic [14].

2.2 Radio Propagation Model

In real vehicular scenarios, nodes can experience packet loss due to signal attenuation caused by multi-path, reflection and distortion between radio waves and the environment. While there are many radio propagation models to determine channel condition in wireless communication environments, they are commonly divided into : deterministic and probabilistic models. The typical deterministic model like Two-Ray ground model has been used due to its simplicity. And the probabilistic model especially Nakagami-m fading model is utilized and suggested by many authors [12-14] as a suitable channel model for highway scenarios due to the good match with empirical data. Therefore, we select the Nakagami-m fading model to perform our simulation.

In order to evaluate the influence of a realistic fading phenomena, we implement Nakagami-m fading model in Qualnet4.0 [18]. Fig 1 shows the probability of successful packet reception rate without interferences from other nodes when the intended transmission range was set as 520m. On one hand, for the deterministic channel model such as Two-Ray ground model, the packet is always successfully received within the transmission range and drops dramatically to zero when out of transmission range. On the other hand, the probabilistic Nakagami-m fading model shows non-deterministic behavior with different value of fading factor m. Furthermore, another key observation is that both m=3, 5 and 7 can have above 80% probability of message reception when the distance is less than 400m.

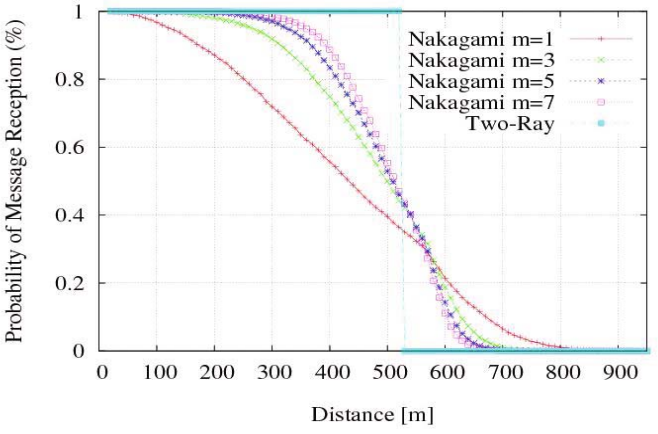


Fig. 1. Probability of Message Reception without interferences from other nodes with different propagation models

2.3 IEEE 802.11p PHY and MAC

In this section, we provide an overview of the overall underlying wireless communication technology of IEEE802.11p used in IVCs. IEEE 802.11p is a variant of 802.11a that modifies its PHY and MAC to support high mobility vehicular commutations. At the PHY layer, IEEE 802.11p reduces the frequency band from 20MHz to 10MHz, which means all parameters values are doubled in time domain comparing with the original 802.11a. By following the current DSRC proposals, we have implemented 802.11p by modifying 802.11a in Qualnet4.0.

With respect to the MAC layer, CSMA-CA based distributed coordination function (DCF) [13] is used as the fundamental strategy in case of ad-hoc communications. Different from the unicast, several things should be taken into consideration when using broadcast communications. First, there is no ACK mechanism to indicate whether the transmission is successful or not at the MAC Layer. Second, there is no RTS/CTS exchange strategy to avoid hidden terminal problem. With a probabilistic propagation model, the hidden node can appear much closer to a sender, which can lead to further performance degradation. Third, there is no automatic retransmission mechanism when packet loss occurs.

Furthermore, Enhanced Distributed Channel Access (EDCA) is adopted in IEEE 802.11p to provide different priorities to access channel. These priorities are classified into four access categories (AC) with their corresponding configuration parameters.

The AIFS[AC] is calculated as equation (1), where SIFS time is 32us and SlotTime is 13us according to the 802.11p standard. The backoff time used for transmission is randomly selected in the range of CWmin and CWmax.

$$AIFS[AC] = SIFS + AIFS[AC] * SlotTime \tag{1}$$

Table 1. Configuration values of different access categories (AC) in EDCA mechanism

AC	CW_{min}	CW_{max}	**AIFS**	T_{AIFS}
0	aCW_{min}	aCW_{max}	9	149us
1	(aCW_{min}+1)/2-1	aCW_{min}	6	110us
2	(aCW_{min}+1)/4-1	(aCW_{min}+1)/2-1	3	71us
3	(aCW_{min}+1)/4-1	(aCW_{min}+1)/2-1	2	58us

In order to provide different priorities, we give different AC categories to the hello beacon message and alert message in our BCF protocol when the simulation (e.g., AC3 for alert message and AC0 for hello beacon message)is performed.

3 Beacon-Based Cooperative Forwarding Scheme

Wireless communication technologies combined with vehicular on-board positioning system, e.g., Global Positioning System (GPS), can support road safety by exchanging hello message periodically (e.g., location, velocity, direction). Especially useful is the fact that upon reception of a periodic beacon message, the vehicle will be aware of its surrounding and capable of detecting potential dangerous situations. Moreover, the BCF protocol combines a set of mechanisms including designating multiple forwarder candidates with different forwarding delays, a helper strategy based on cooperative forwarding and several optimizations to discard unnecessary rebroadcasting packets.

3.1 Hello Beacon Message

Our proposed protocol, called the Beacon-based Cooperative Forwarding (BCF) scheme designs the forwarding strategy based on neighboring information by periodically exchanging a hello message. In the proposed BCF scheme, we design the format of *hello message* as follows:

hello message: {*ID, sequence, position, direction, velocity*}

Where ID stands for the identifier (e.g., MAC address) of node, sequence is the only identification to distinguish different hello message and *position, direction, velocity* are the node's own information when sending the hello message. Once the node receives *hello message* from the neighbors, it will update its own *neighbor table* illustrated by the following data structure:

neighbor table: {*ID, sequence, position, direction, velocity,timeout*}

However, due to the high mobility, the beacon messages about neighbors information can become out of date, which has a significant impact on selecting the forwarder candidates. Considering this characteristic, *timeout* is used in *neighbor table* for maintaining the latest forwarder information, which means that the

timeout is expired, this node information should be deleted from the *neighbor table* because it may not be accurate any more. While in periodic beacon schemes, the *timeout* is a fixed value depending on the beacon generation frequency. Here a mobility predication-based beacon strategy is proposed to decide the *timeout* value according to the nodes location and velocity information. The core principle here is to estimate the *timeout* value by predicting the maximum duration time when the two adjacent nodes move out of the communication range from each other.

Without loss of generality, we assume that node i is following node j. We use the notion of link lifetime LL (i, j, t) as a connection between two nodes i and j to indicate the time node i will remain in the transmitting range of node j. The link lifetime between the two nodes could be computed from the current distance D(i, j, t), relative speed RS and transmitting range R, which are denoted by the following formula:

$$LL(i, j, t) = (R - D(i, j, t))/RS(i, j, t) \tag{2}$$

If LL (i, j, t) ¡ certain timeout threshold (e.g, 3s), the timeout value is set as LL (i, j, t); otherwise, use the original timeout value. By setting appropriate *timeout* in this way, the strategy can prevent the beacon information becoming obsolete as well as control the beaconing load.

Since some authors [15] are concerned that the beacon can aggravate the channel congestion, here we give a calculation analysis on how much bandwidth will be occupied by the beacon message. The average among of beaconing load (BL) within a nodes transmission range can be computed as follows:

$$BL = VehicleDensity * 2R * Packet * BeaconSize \tag{3}$$

When *VehicleDensity* is 24 vehicles/km and 54 vehicles/km separately taking into account the multiple lanes (the vehicle density used in our simulation scenarios), transmission range R is 520m, the average *packet generation* frequency is 1 packets/s and hello message *BeaconSize* is 0.5k bits/packet. Therefore, we can obtain a maximum BL of less than 0.3 Mbps, which is far from aggravating network load compared to a 3 Mbps bandwidth.

3.2 Multiple Forwarder Candidates Designation

Fig. 2 shows the basic operation of BCF protocol. When V1 detects a danger event on the road, it disseminates an alert message to all surrounding nodes within a certain area (e.g., 2 3km). The header of alert message may contain two designated forwarder candidates, such as V4 and V5 shown in red. Only these specified candidates can rebroadcast the alert message. And the nodes that are not specified like V2 and V3 only receive the alert message and perform some actions to avoid danger. In order to prevent contention between the candidates, the forwarding delay of each candidate is differentiated according to its relative distance to the sending node. By doing this, the furthest node has the smallest forwarding delay. Therefore, V5 may be the next forwarder since its location is

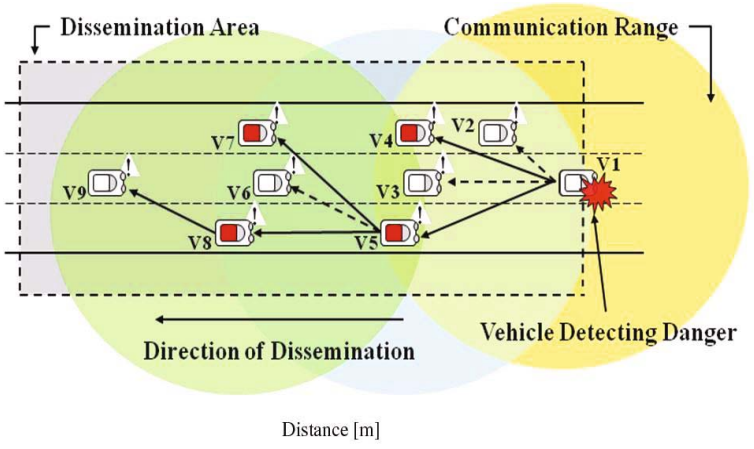


Fig. 2. Illustration of the specification of forwarding candidates after accident detection in highway. Note that the red nodes are specified forwarding candidates.

further than V4, and V4 will stop rebroadcasting when the duplicated packets from V5 are recived. Then V5 will specify its own forwarder candidates such as V7 and V8 for the next rebroadcasting.

Obviously, only the vehicles behind the sending node can benefit from receiving the safety message, therefore, we mainly focus on choosing the candidates in the backward area with the same direction from the sender. Additionally, in section 2 we observed that the distance between the sender and receiver is significantly shorter than the communication range, due to the hidden terminal problem and probabilistic propagation model (e.g., above 80% probability of message reception when the distance is less than 400m when the communication range is 520m). Thus we limit the length of the forwarding area to less than the communication range to guarantee high reliability. Motivated by the above considerations, we bring up the conception of forwarding zone and forwarding area as follows:

– *Forwarding Area* (fwd area): is the covered dissemination area within one-hop transmission.

– *Forwarding Zone* (fwd zone): is the smaller area within the forwarding area, especially with vehicles located in forwarding zone having the same moving direction as the sender.

Based on the *Forwarding Zone* conception, the following *forwarder candidate* selection and priority decision rule mechanisms are proposed in this paper.

– *Forwarder Candidate Selection*: when a node wants to broadcast the alert message with its own forwarder candidates, it will search its neighbor table

to find the next hop forwarding nodes in the forwarding zone, which should satisfy the following conditions: i) nodes behind it according to location information. ii) nodes moving in the same direction. iii) the selected forwarder candidates number is less than the maximum number of forwarders.

– *Priority Decision Rule*: the priority of forwarder candidates are determined by relative distance information with the principle of the farthest node having the highest priority.

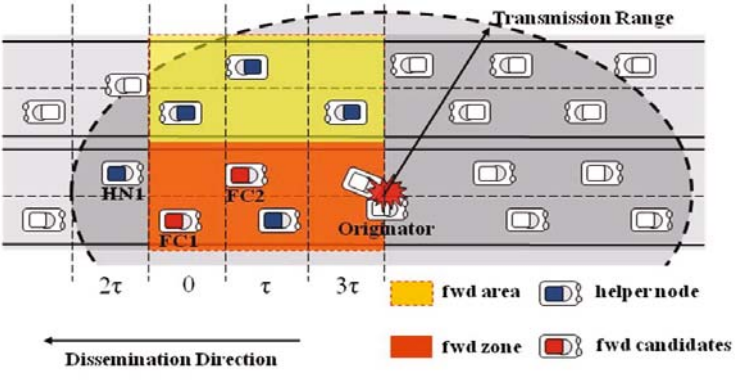


Fig. 3. Illustration the conception of forwarding zone and forwarding area, forwarder candidate and helper node

3.3 Cooperative Forwarding Scheme

Based on previous studies [16], we identify the need of a mechanism to prevent random packet loss due to the hidden terminal problem, radio attenuation and heavy link load in dense traffic situations. Thus, in order to prevent packet loss and guarantee high reachability, we have proposed a cooperative forwarding strategy to help forwarding when all the specified forwarder candidates fail to transmit the message. The key idea of this strategy is nodes that receive safety messages are separated into two categories by playing different roles in the forwarding procedure. As shown above, when the node in the forwarding area receives a safety message, first, it checks the header information to decide whether it is the sender designated forwarder candidate or not. As the *forwarder candidate*, it prepares a rebroadcasting with its own *forwarding delay* based on the header information, which includes two fields: the *number of forwarder* and the *forwarder ID list* arranged through priority. The forwarding delay can be easily calculated as forwarder priority sequence multiplies one-hop delay . For example, in Fig. 3, when the *number of forwarder* is 2 and *forwarder ID list* is FC1, FC2, the FC1 and FC2 forwarding delay is 0* ms and 1* ms separately.

Table 2. Cooperative Forwarding Scheme with forwarder candidates and helper nodes

```
/* Upon receiving a safety message from neighbor, decide whether itself is the forwarder candidate
or not by checking the header information.*/

01:   IF Forwarder Candidate
02:       Add forwarding delay according to the priority sequence
03:       IF forwarding delay is expired
04:           Search neighbor table to find own forwarder candidate
05:           IF neighbor table is empty ;
06:               Start contention-based forwarding scheme

07:           ELSE /* multiple forwarders exist in neighbor table*/
08:               Select forwarder candidates according to forwarder candidate selection.
09                Set candidates priority by using priority decision rule.
10:               Replace with node own forwarder candidates
11:   ELSE Helper Node
12:       Add maximum waiting time= one-hop delay * number of forwarding candidates.
13:       IF forwarding delay is expired
14:           Start contention-based forwarding scheme
15:   END
/* Duplicated Packet Detection (DPD) count the received duplicated packets during the forwarding delay.
If the counting value is larger than certain threshold, stop fowrading.*/

16:   IF Received duplicated packet ¡ threshold
17:       Rebroadcast the packet immediately
18:   ELSE
19:       Discard the packet, stop forwarding.
20:   END
```

Otherwise, the forwarding delay of help node is set with the maximum waiting time which can be denoted as follows:

$$Maximum\ waiting\ time = \tau * number\ of\ forwarder \tag{4}$$

In this period, if no duplicated packet is received, it means that all the specified forwarder candidates fail to transmit the message. Therefore, the help node will start to rebroadcast the message by exploiting the slotted-1 scheme [4]. Finally, the forwarding delay of furthest node (e.g., HN1 in Fig. 3) is set as 2* ms by following equation.

$$forwarding\ delay = \tau * \lceil N_s(1 - min[d_{ij}, R]/R \rceil \tag{5}$$

3.4 Optimization

In order to discard unnecessary rebroadcasting packets, our scheme has a duplicated packet detection (DPD) procedure, which counts the received number of duplicate packets during the forwarding delay. If the counting value is larger than a certain threshold, it will stop the forwarding procedure. Contrary to other broadcast protocols based on a fixed parameters value, the DPD threshold is changed dynamically depending on the estimation of vehicle density according to neighborhood information.

4 Simulation and Performance Analysis

4.1 Highway Scenarios

The evaluated vehicular scenario is configured according to the VanetMobiSim [17] mobility generation tool.

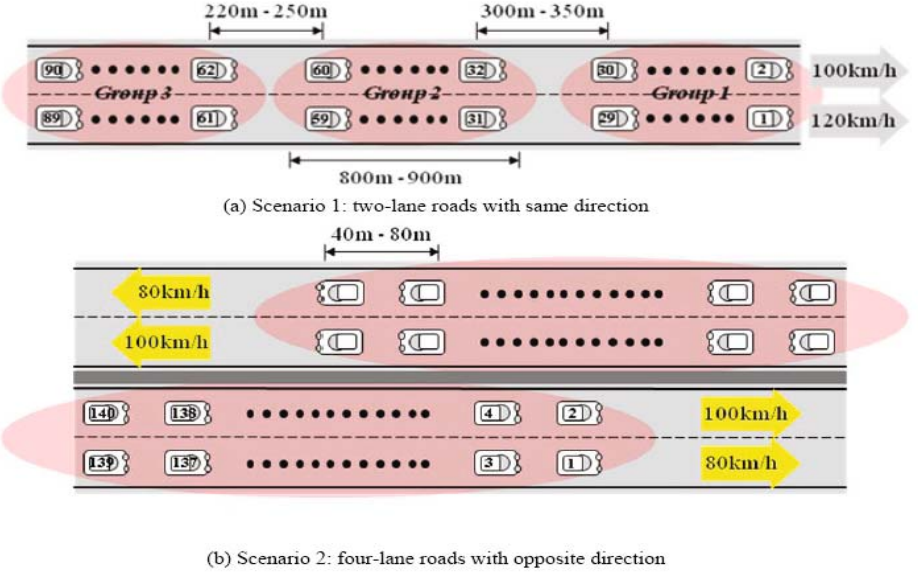


Fig. 4. Highway Scenarios used to evaluate the performance of proposed BCF scheme

All 90 nodes in Scenario 1 are divided into three groups with a group distance between 220 350m. The selected case for this study consists of an average density of 12 vehicles/km in each lane with a driving speed of 100km/h or 120km/h, which corresponds to a medium vehicular density and fast-moving highway traffic.Scenario 2 corresponds to a dense traffic model, which consists of 280 vehicles placed in a 4 parallel lanes in opposite directions.

Given the vehicular safety applications considered earlier, we assume that the alert messages are generated by the foremost four nodes (e.g., node 1, 2, 3, 4), which may detect the danger first and transmit the alert message simultaneously. Each source node generates a 500 bytes packet every 200ms. Although the simulation time is 12s, we mainly focus on analysis of the message transmission situation during one second after the message is generated, which is the critical time for the drivers to take some actions such as braking.

4.2 Simulation Setup

In all simulations, the transmission range is set to 520m with a data rate of 3Mbps in IEEE802.11p. The compared schemes (e.g. Pure Flooding, Weighed-p,

Table 3. Simulation parameter in Qualet 4.0

Parameter	Value
Tx Range	Intended to 520m without fading model
Data Rate	3Mbps (OFDM 10Mhz)
PHY	IEEE 802.11p, Nakagami m =5
MAC	EDCA (AC0: hello, AC3: safety message)
Network	PF/DDB/Slotted-1/Weighted-p/BCF

Table 4. Key parameters of BCF scheme

Parameter	Value
Hello Interval	Periodic 1 second
Allowed Hello Loss	3
Number of Forwarder	3
Minimum One-hop Delay	2ms
Number of Slot	5
Nakagami-m fading factor	5
Forwarding Zone	400m

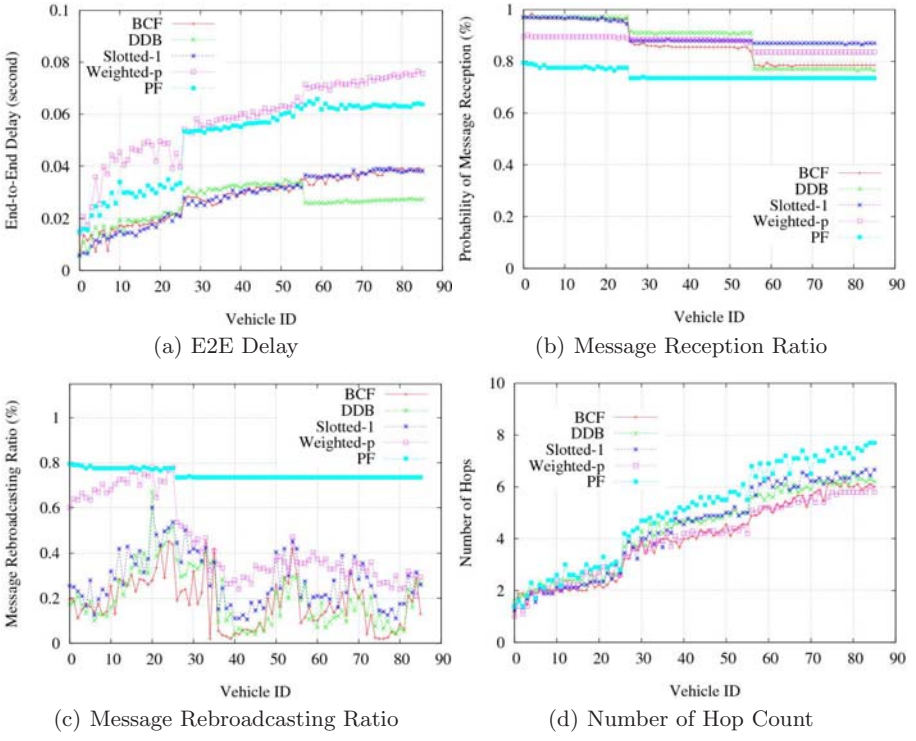
Slotted-1 and DDB) are configured as the authors recommend(e.g., Max Waiting Time in DDB is 20ms, both Slotted-1 and Weighted-p's Average One-hop Delay is 4ms). For parameters of BCF protocol as shown in Table 3, the minimum one-hop delay is 2 ms which can be calculated as PacketSzie plus AddedHeader divides DataRate. Besides,the MAC Contention Delay should be consided. It is worth mentioning that the one-hop delay used in Weighted-p and Slotted-1 is 4ms instead of 2ms, which is a rough estimated value greater than the minimum one-hop delay.

According to the previous analysis using the Nakagami-m fading channel model, we can observe that it will achieve above 80% of message reception when the distance is less than 400m with a communication range of 520m and a fading factor m is 5. Thus, it is reasonable that the width of Forwarding Zone is set as 400m to assure a high message reception ratio. The configuration details are summarized in Table 4.

4.3 Performance Analysis

In this section, we compare the performance of the proposed broadcast schemes with conventional contention-based methods. We have implemented and evaluated the proposed BCF schemes and compared contention-based protocols in the Qualnet4.0. The results were averaged over 30 times by changing the time seed and given with a 95% confidence interval.

Another important task in simulation is the proper evaluation and interpretation of the obtained data. In this part, we introduce the main metrics utilized to evaluate the performance of the proposed BCF schemes. The four quantitative metrics includes:Maximum End-to-End Delay,Message Reception Ratio,Message Rebroadcasting Ratio and Number of Hops.

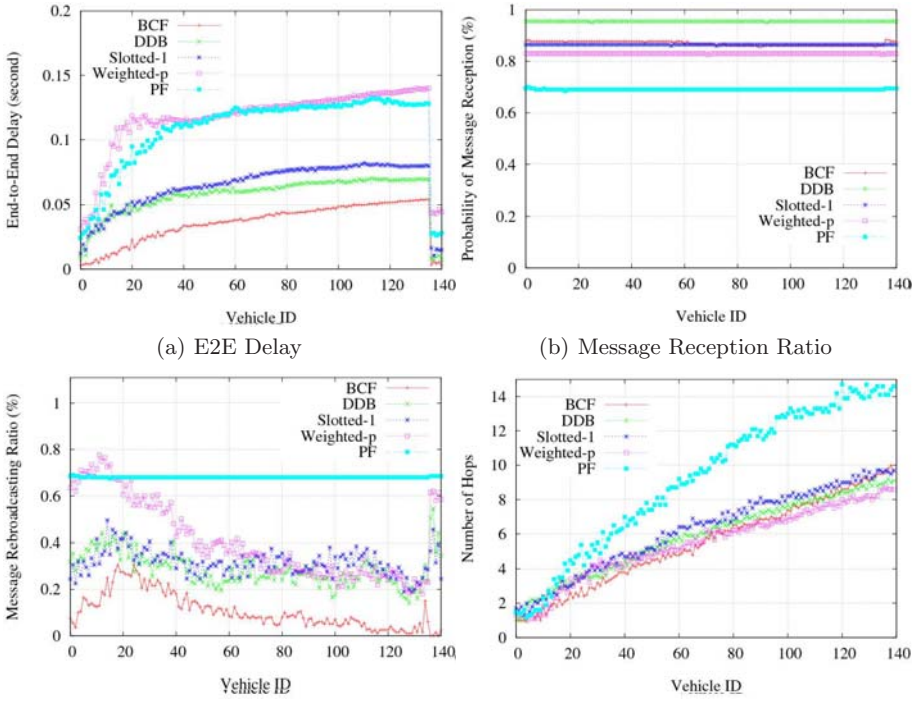


(a) E2E Delay (b) Message Reception Ratio

(c) Message Rebroadcasting Ratio (d) Number of Hop Count

Fig. 5. Scenario 2 Simulation Results includes End-to-End Delay, Message Reception Ratio, Message Rebroadcasting Ratio and Number of Hops

- *Maximum End-to-End Delay*: Since in broadcasting schemes, all nodes will receive the message except the source nodes because the destination address is broadcasting address. Thus, the delay should be defined as the maximum latency between the source and the other nodes received by it.
- *Message Reception Ratio*: The ratio is measured as the number of packets which are received successfully at each node divided by the total packet sent by source. This metric represents the reception ratio of messages without retransmission.
- *Message Rebroadcasting Ratio*: The ratio of total rebroadcasting packets in the network. Intuitively, the message rebroadcasting ratio depends on the number of retransmitting nodes; for example, if every node decides to retransmit, as in brute force 1-persistence, the Message Rebroadcasting Ratio equals to 100%. Obviously, the smaller the message rebroadcasting ratio, the less contention among nodes.
- *Number of Hops*: The number of network nodes relayed between the source node and the destination node. Normally, a large number of hop counts can lead to longer end-to-end delay.



(a) E2E Delay (b) Message Reception Ratio

(c) Message Rebroadcasting Ratio (d) Number of Hop Count

Fig. 6. Scenario 2 Simulation Results includes End-to-End Delay, Message Reception Ratio, Message Rebroadcasting Ratio and Number of Hops

As shown in Fig. 5 (b), almost every scheme except pure flooding can achieve above 80% message reception ratio. One thing should be noticed is that the safety message loses nearly 10% when the packets are forwarded from group to group. As mentioned before, the Nakagami-m fading channel experiences packet loss dramatically as the distance increases. This is certainly caused by the nearly 300m distance gap between each group.

In Fig. 5 (c) we can observe that pure flooding has a message rebroadcasting ratio of around 80%. Obviously, a high rebroadcasting ratio can cause high contention at the link layer, and hence the risk of E2E delay is higher due to more hop counts. Additionally, the message reception ratio is also affected by the packet collision due to a hidden terminal problem. Therefore, Weighted-p, DDB and Slotted-1 can effectively suppress the contention by setting additional dynamic forwarding delay based on the distance from the sender. However, in medium traffic density, since the BCF exploits contention-based scheme in the cooperative forwarding strategy, a similar rebroadcasting rate is shown. Besides, all the schemes has the same number of hopcount.

Given that the node density in Scenario 2 is twice that of Scenario 1, much more contention can lead to further performance degradation. As shown in Fig. 6 (a) and

(b), BCF, DDB and Slotted-1 show acceptable performance in terms of E2E Delay (less than 100ms) and message reception rate (over 80%), which can achieve the requirement of safety-related applications.

In particular, the BCF shows a minimum E2E delay because the designated forwarder candidates can effectively mitigate the contention of the wireless medium. Another key observation from the Fig. 6 (c) is that message rebroadcasting ratio of BCF is less than twice of other contention-based scheme such as Slotted-1, while keeping the same message reception ratio compared with the Slotted-1. Therefore, the proposed BCF protocol shows a superior performance in different traffic situation. From the figure of Number of Hop Count, we know that even though we limit the forwarding range in BCF, it has almost the same hop count as other scheme, which explains the lower E2E delay in BCF scheme.

5 Conclusions and Future Works

In this paper, we proposed the BCF protocol, which specifies multiple forwarder candidates for fast dissemination of safety messages and adopts a cooperative forwarding strategy to prevent packet loss. We have compared the performance of the proposed BCF with the existing broadcast schemes (i.e., Pure Flooding, Weighted-p, Slotted-1 and DDB) in the realistic channel model and suitable vehicular scenarios. From simulation results, we can observe that the proposed scheme efficiently utilizes the network resource and satisfies the requirements of vehicular safety applications.

In the future, we will focus on relative positioning techniques to solve aberration of GPS in the urban scenario and control the beaconing load by cross-layer optimization.

Acknowledgements

This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2009-(C1090-0902-0016)).

References

1. Krishnan, H.: Vehicle Safetey Communications Project. CAMP Vehicle Safety Communications Consortium (2006)
2. Nakajima, S., Ino, S.: A Preliminary Study of MR Sickness Evaluation Using Visual Motion Aftereffect for Advanced Driver Assistance Systems. Engineering in Medicine and Biology Society (2007)
3. Marc Torrent Moreno.: Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment: Challenges, Systems and Protocols. In: Dissertation (2007) ISBN: 978-3-86644-175-0

4. Bai, F., Krishnan, H., Sadekar, V., Holland, G.: Towards Characterizing and Classifying Communication-based Automotive Applications from a Wireless Networking Perspective. In: IEEE workshop on Automotive Networking and Applications Vehicular Technology (2006)
5. Kwak, D.Y., Bai, S.N., Lee, S.W., Jung, J.I., Oh, H.S.: Sender-designated Alert Message Propagation in IVC. In: WICON (2008)
6. IEEE Std 802.11p Wireless Lan Medium Access Control (MAC) And Physical Layer(PHY) Specifications (2007)
7. Fracchia, R., Meo, M., Rossi, D.: IVCs: To Beacon or Not To Beacon? In: Proc. of the Autonet06 at IEEE Globecom 2006 (2006)
8. Ozan, K., Wisitpongphan, N.: On the Broadcast Storm Problem in Ad hoc Wireless Networks. In: 3rd International Conference BROADNETS 2006, San Jose, California, USA (2006)
9. Heissenbttel, M., Braun, T.: Optimized Stateless Broadcasting in Wireless Multihop Networks. In: INFOCOM (2006)
10. LeBrun, J., Chuah, C.N., Ghosal, D., Zhang, H.M.: Knowledge-Based Opportunistic Forwarding in Vehicular Wireless Ad Hoc Networks. In: IEEE VTC 2005 (2005)
11. Tonguz, O., Wisitpongphan, N.: Broadcasting in IVC. In: 2007 Mobile Networking for Vehicular Environments (2007)
12. Torrent-Moreno, M., Schmidt-Eisenlohr, F.: Effects of a realistic channel model on packet forwarding in vehicular ad hoc networks. In: WCNC (2006)
13. Simon, M., Alouini, M.: Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. John Wiley & Sons, Chichester (2000)
14. Keli, Z., Zhefeng, S.: Simulation of Nakagami fading channels with arbitrary cross-correlation and fading parameters. IEEE Transactions in Wireless Communications (2004)
15. Rossi, D., Fracchia, R.: VANETs: Why Use Beaconing at All? ICC (2008)
16. Yin, J., Elbatt, T.: Performance Evaulation of Safety Applications over DSRC Vehicular Ad Hoc Networks. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (IVC), USA (2004)
17. VanetMobiSim, http://vanet.eurecom.fr
18. Qualnet 4.0, http://www.scalable-networks.com

Author Index